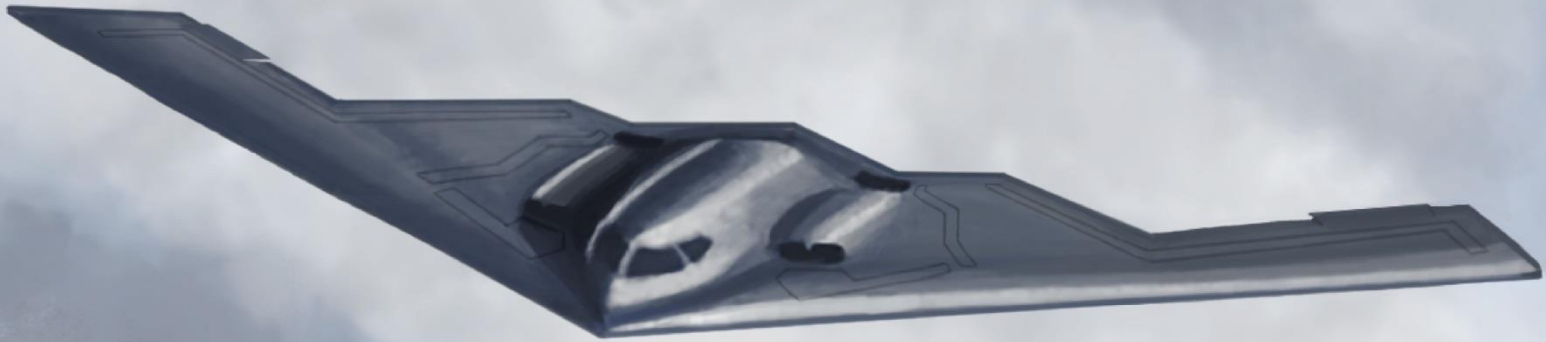


A course of mathematics



Book I

Construction of numbers,
length and area.

Naumov Ivan

Book I. Construction of numbers, length and area.

ISBN 978-952-94-0570-1
ISBN 978-952-94-0571-8
ISBN 978-952-94-0572-5
ISBN 978-952-94-0573-2

Copyright © Naumov Ivan, 2018.

Illustrator, designer
Gudalova Tatiana

Finland 2018

Preface

The 1-st book is done to provide a complete construction of numbers, length and area.

It is obviously the most reasonable way to start a course of mathematics. Almost everyone knows that when we operate with numbers, we do it according to the certain rules.

Unfortunately, there is never any explanation of where these rules came from, despite the fact that it is a very important question, to say the least.

Really, almost anyone knows the “sign rules” $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$, $(-a) \cdot (-b) = a \cdot b$ [A], or a commutative law $a \cdot b = b \cdot a$ [B], or an associative law $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ [C].

But it's not typical of people to ask: “Why are these laws true?”.

If someone gets a “math education”, he will be told that the real numbers R form a “field” and even a “complete field”, and that's where all the properties like [A],[B],[C] came from. But it explains nothing, because it immediately leads to the question: “Why do the real numbers R form a field?”. And the better person knows math, the easier he can understand that there must be some good explanation of all these properties, as they aren't obvious at all. So, there are “infinitely many” real numbers. Why do all of them without any exceptions obey to the certain rules? Why can we take some line and compare exactly one (appropriate) real number to every point of that line, such that every real number will be compared to some point? I've never seen any students curriculum where any of these fundamental questions are normally explained.

Is it so because it is something obvious or something insignificant? No, in reality, not at all.

Eventually, there exist only one reasonable way to answer all these questions - to provide a complete and clear construction of the field R . We will start from the simplest basic objects and then, step by step, we will be building real numbers, and during the process we will check straightly all their properties, without accepting any of them for granted. As far as I'm concerned, the numbers construction $N \rightarrow Z \rightarrow Q \rightarrow R \rightarrow C$ is one of the most amazing and the most important part of mathematics. There exist several known approaches to such construction, and some of them have serious flaws, because if we follow them, most of the properties of numbers will stay unexplained. The main goal of this book is to provide the most convenient construction, where definitions are clear and there is a strict logical structure, there are no “gaps” and “uncertainties”, and there are no inconvenient and protracted proofs at all. My main goal was to give only a good quality information and to make the narrative consecutive and clear.

All The Best,

Naumov Ivan

Table of contents

Natural numbers	5
Groups, Rings, Fields.....	33
Matrixes.....	46
Integer numbers.....	53
Rational numbers.....	73
Sequences and limits.....	84
Real Numbers.....	93
Construction of length.....	130
Construction of area.....	149
Angles.....	165
Literature.....	171

I express my sincere gratitude to:

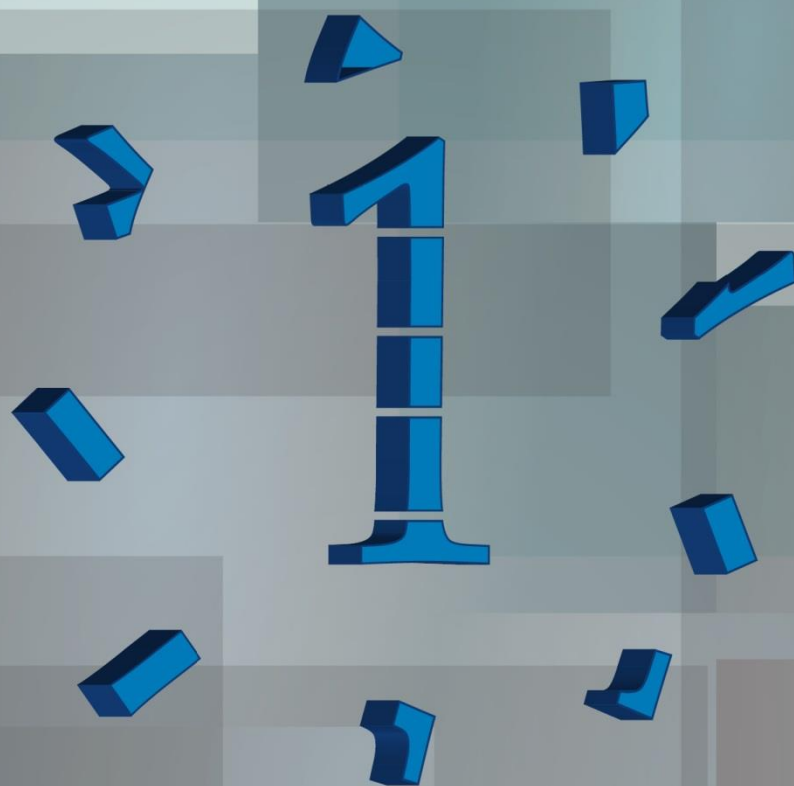
Galochkin Alexandr Ivanovich

Drutsa Alexey Valerievich

Kozko Artem Ivanovich

Because their lectures and seminars made me interested in math
and formed my approach to this subject.

I also would like to thank **Alexander Bebris**, as his educational web site and the project
“English Galaxy” provided a great course of English grammar, which is essential for writing.



*Natural
numbers*

Basic objects and notions.

Def: a set A is any collection of unique objects, every object of A must be understood as exceptional and different from any other object of A . Any separate objects in such collection must be considered as **different** objects.

We use small letters a, b, c, d, \dots to denote objects of any set.

Every small letter always denotes one object of a set. It is allowable to use different letters a, b to denote the same object. And if both letters a, b denote the same object, we must write $a = b$. If letters a, b denote different objects, we must write $a \neq b$.

We will usually work with sets of symbols, like the set of natural numbers $\{1, 2, 3, 4, \dots\}$ - notice that every symbol of this set is unique. And we can use small letters a, b, c, d, \dots to denote some natural numbers. If letters a, b both denote the same natural number, then we must write $a = b$, if a, b denote different natural numbers, we must write $a \neq b$.

Sets A and B are equal $A = B$ if they consist of exactly the same elements.

In any other case we write $A \neq B$.

If A contains a , we write $a \in A$. If A doesn't contain a , we write $a \notin A$.

When $a \in A$ we say " a belongs to A ", when $a \notin A$ we say " a doesn't belong to A ".

The writing $B \subset A$ means " B is a subset of A ", it means that every element of B belongs to A .

For convenience we define an empty set \emptyset - the set without any elements.

And by definition, any set A contains an empty set \emptyset as a subset, $\emptyset \subset A$.

Exercise. If $A \subset B$ and $B \subset A$, then $A = B$.

Example. Any set that consists of elements a, b can be written as $\{a, b\}$, or $\{b, a\}$.

A set that consists of elements a, b, c can be written as: $\{a, b, c\}$, or $\{a, c, b\}$, or $\{b, a, c\}$, or $\{b, c, a\}$, or $\{c, a, b\}$. The positioning of elements inside the brackets $\{\dots\}$ is irrelevant.

Def. Let A and B are any sets. The intersection of A and B is the set

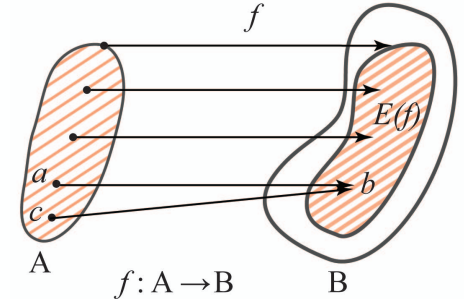
$A \cap B = \{a \mid a \in A \text{ and } a \in B\}$ which consists of all the elements that belong to A and to B .

The union of A and B is the set $A \cup B = \{a \mid a \in A \text{ or } a \in B\}$ which consists of all the elements that belong to A or to B (**Notice:** if a is a common element of A and B , we do not include it twice in $A \cup B$, only once). And finally, the difference of A and B is the set

$A \setminus B = \{a \mid a \in A \text{ but } a \notin B\}$ which consists of all the elements that belong to A , but do not belong to B .

Def. A and B are any sets. And f is any rule such that: for every element $a \in A$ the rule f compares exactly one element $b \in B$, then f is called a function (or a mapping) from A to B . And we denote it like $f : A \rightarrow B$. Let $a \in A$ and f compares to a some element $b \in B$, then we write $f(a) = b$. And we say that " b is an image of a " and " a is a preimage of b ".

So, when we write $f : A \rightarrow B$, we mean that for every $a \in A$ some element $b \in B$ is compared. But there is no requirement [pict1] that every element $b \in B$ is compared to some $a \in A$, some elements of B may not have any preimage in A . The set A is called a **domain** of f , and we can write $D(f) \equiv A$. The set $E(f) \equiv \{b \in B \mid \exists a \in A : f(a) = b\}$ - is a subset of B , and $E(f)$ is called an image of f . Notice that $E(f)$ mustn't coincide with B , it just belongs to B . In general, f may transfer different elements $a, c \in A$ into the same $b \in B$, so it can "glue together" different elements of A [pict1].



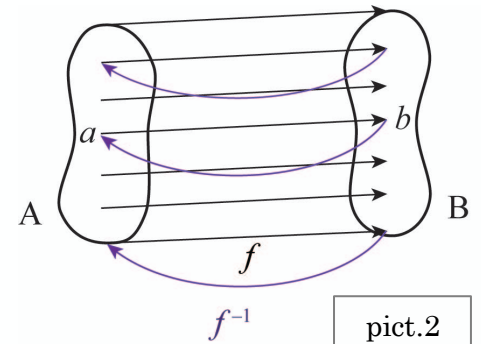
pict.1

In the case when f doesn't "glue together" any elements of A (I.e., for any $a, c \in A$: if $a \neq c \in A$, then $f(a) \neq f(c) \in B$), we say " f maps A into B ".

If B is "completely covered" by f (for every $b \in B$ there exist some $a \in A$ such that $f(a) = b$), then we say " f maps A onto B ".

If f does not "glue together" elements of A and "covers B completely" (f is into and onto mapping), then we say that " f is **one-to-one mapping** from A to B ".

Only when f is one-to-one, we can define the inverse mapping $f^{-1} : B \rightarrow A$ [pict2], for any $b \in B$: if $b = f(a)$, then $f^{-1}(b) \equiv a$.



pict.2

Exercise. If f is one-to-one, then f^{-1} is also one-to-one.

Also, for any $a \in A$ we have $f^{-1}(f(a)) = a$ and for any $b \in B$ we have $f(f^{-1}(b)) = b$.

Let we have some mapping $f : A \rightarrow B$. In order to show that f is one-to-one we need:

[Step1] To show that f covers B : for any $b \in B$ there exist some $a \in A$ such that $f(a) = b$.

[Step 2] To show that f doesn't "glue together" elements of A . Usually it can be done in the next way: we fix any elements $a \neq c \in A$ and we assume that $f(a) = f(c)$. From the last equality " $f(a) = f(c)$ " we try to derive (by using some properties of a concrete mapping f) that $a = c$, it contradicts to our initial requirement $a \neq c$. And therefore, our assumption " $f(a) = f(c)$ " was false and $f(a) \neq f(c)$.

Def. A and B are any sets. If there exist any one-to-one mapping $f : A \rightarrow B$, then we say " A is equivalent to B ", and we write $A \approx B$.

If $f : A \rightarrow B$ is one to one, then $f^{-1} : B \rightarrow A$ is one-to-one, therefore $A \approx B \Leftrightarrow B \approx A$.

And we can just say "sets A and B are equivalent".

If there is no any one-to-one mapping $f : A \rightarrow B$, then we say " A is not equivalent to B ".

General definition. Ω is a set of any kind. And " \approx " is some condition that may be true for some pairs $a, b \in \Omega$. And for any $a, b \in \Omega$ exactly one of the next cases is true:
 $a \approx b$ (the condition \approx is true for the pair a, b) **or** $a \not\approx b$ (the condition \approx is not true for the pair a, b).
And also [A] $a \approx a$ (for any $a \in \Omega$) (**reflexivity**), [B] If $a \approx b$, then $b \approx a$ (**symmetricity**),
[C] If $a \approx b$ and $b \approx c$, then $a \approx c$ (**transitivity**). Then " \approx " is called an equivalence relation on Ω

Example. Ω is a set, and Ω is divided into some sets

$A_\mu \parallel \mu \in M$ [pict3] without common elements:

$A_\mu \cap A_\eta = \emptyset$ if $\mu \neq \eta$. Let's define that elements a, b are

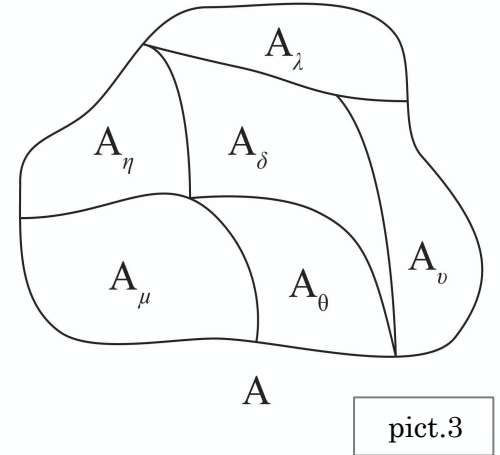
equivalent $a \approx b$ if and only if both a, b belong to

the same set A_δ . Then " \approx " is an equivalence relation on Ω .

Really, $a \approx a$ for any $a \in \Omega$, if $a \approx b$, then both a, b belong to

some set A_δ and therefore $b \approx a$. If $a \approx b$ and $b \approx c$, then a, b, c

belong to the same set A_μ and therefore $a \approx c$.



pict.3

The main property of any equivalence relation. Ω is a set, then any equivalence relation " \approx " on Ω divides Ω into disjoint sets, which are classes of equivalent elements.

Proof. Let we have some equivalence relation " \approx " on Ω . For every $a \in \Omega$ let's consider the class $A_a = \{all \delta \parallel \delta \approx a\}$. The set A_a includes all the elements $\delta \in \Omega$ which are equivalent to a .

Let's fix an arbitrary pair of sets A_a and A_b . Let's show that exactly one of the next cases is true:

$A_a \cap A_b = \emptyset$, **or** $A_a = A_b$. If $A_a \cap A_b = \emptyset$, then we have the first case. Let $A_a \cap A_b \neq \emptyset$,

then there exist some δ such that $\delta \in A_a$ and $\delta \in A_b$. From the condition $\delta \in A_a$ follows that

$A_\delta = A_a$. From the condition $\delta \in A_b$ follows that $A_\delta = A_b$. Then $A_a = A_b$. Any element $a \in \Omega$

belongs to some class A_a , and any classes A_a, A_b coincide completely, or do not have any common elements at all, then Ω is divided into disjoint sets. Everything is proved.

Def. A set Ω is called an **ordered set** if there exist some condition "<" that may be true for some pairs $a, b \in \Omega$. If "<" is true for some pair a, b , we write $a < b$. And also:

[A] For any $a, b \in \Omega$ only one of the next cases is true: $a = b$, **or** $a < b$, **or** $b < a$.

[B] "<" is transitive: if $a < b$ and $b < c$, then $a < c$.

In such case we say that "<" is an order relation on Ω . And we can write $(\Omega, <)$ instead of Ω ,

in order to emphasize that there is an order on Ω . We must agree that in the case $a < b$ we will

say " a is less than b ", or " b is greater than a ". We also need to agree that the writings $a < b$

and $b > a$ are equivalent. If $a < b$ or $a = b$, we will write $a \leq b$ and say " a is not greater than b ", or " b is not less than a ".

Def. $(A, <)$ and $(B, \tilde{<})$ are some ordered sets. If exist one-to-one mapping $f : A \rightarrow B$ such that:

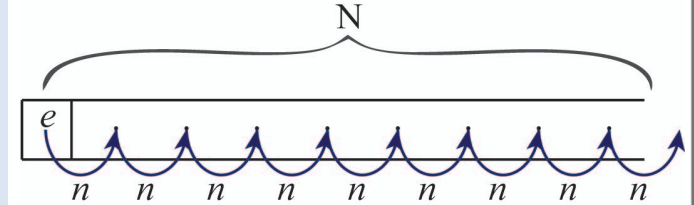
$a < b$ (in A) $\Rightarrow f(a) \tilde{<} f(b)$ (in B), then we say that $(A, <)$ is isomorphic to $(B, \tilde{<})$, and we write

$A \cong B$. It's very easy to show that: $A \cong B \Leftrightarrow B \cong A$ and we can say "ordered sets A, B are isomorphic".

Natural numbers.

Def. \mathbb{N} is a nonempty set. There exist the element $e \in \mathbb{N}$, which is called “one”, and one-to-one mapping $n: \mathbb{N} \rightarrow \mathbb{N} \setminus \{e\}$. For any element $a \in \mathbb{N}$, the element $n(a) \in \mathbb{N}$ is called “next to a ”. And the induction axiom is true in \mathbb{N} [pict4].

| Induction axiom | Let M is a subset of \mathbb{N} , and $[A]$, $[B]$ are true.
 $[A] e \in M$ $[B]$ If some a belongs to M , then $n(a)$ also belongs to M .
 Then there must be $M = \mathbb{N}$.



pict.4

Then \mathbb{N} is called a set of natural numbers and elements of \mathbb{N} are called natural numbers.

It's easy to see that the set of natural numbers is not an ordinary set, it is a structure which consists of the (set) + (mapping) + (induction axiom).

Let's provide an example which satisfies to the given definition. It's very easy to do, let's take the letter A and let's consider the set of “words” $\mathbb{N} \equiv \{A, AA, AAA, AAAA, AAAAA, AAAAAA, \dots\}$.

Our set comprises all the possible “words” with only one letter A . We designate $e \equiv A$.

And we also define one-to-one mapping $n: \mathbb{N} \rightarrow \mathbb{N} \setminus \{A\}$: for any word $AA \dots A$ we compare the word on the right of it, so $n(A \dots A) = A \dots AA$. Then n is one-to-one mapping $\mathbb{N} \rightarrow \mathbb{N} \setminus \{A\}$.

Let's check that the induction axiom is true in \mathbb{N} , really let's assume that $[A]$ and $[B]$ are true for some set $M \subset \mathbb{N}$. From $[A]$ follows that $A \in M$, from $[B]$ follows that if some word belongs to M , then the word on the right of it also belongs to M . From $[A]$ we have $A \in M$, then from $[B]$ follows that $AA \in M$, then $AAA \in M$, then $AAAA \in M$ and etc. And therefore, M must contain every word $A \dots A$, then $M = \mathbb{N}$. So the induction axiom is true. And our set \mathbb{N} is a set of natural numbers.

Similarly $\mathbb{N}_B = \{B, BB, BBB, BBBB, \dots\}$ is also a set of natural numbers. As letters A and B are in fact different symbols, then the sets \mathbb{N} and \mathbb{N}_B are different sets. But it's very easy to see that these sets have the “same structure”. In math such sets are called isomorphic.

The main theorem. Any set of natural numbers \mathbb{N} can be written as:

$$\mathbb{N} \equiv \{e, n(e), n(n(e)), n(n(n(e))), n(n(n(n(e)))) \dots\}.$$

Let's assume that this theorem is true. From this theorem we see that if \mathbb{N} is written like $\mathbb{N} \equiv \{e, n(e), n(n(e)), \dots\}$ (each next element is an image (after the mapping n) of it's left neighbor), then for any $a \in \mathbb{N}$ the element $n(a)$ is literally next to a .

Really, if $a \in \mathbb{N} \Rightarrow a = n(\dots n(e) \dots)$, then $n(a) = n(n(\dots n(e) \dots))$ stays on the right of a and $n(a)$ is literally next to a .

Let now N_A, N_B are some sets of natural numbers. Then, according to the **main theorem**:

$$\begin{aligned} A &\equiv \{e_A, n(e_A), n(n(e_A)), n(n(n(e_A))), n(n(n(n(e_A)))) \dots\} \\ B &\equiv \{e_B, n(e_B), n(n(e_B)), n(n(n(e_B))), n(n(n(n(e_B)))) \dots\} \Rightarrow \\ \Rightarrow &\begin{array}{cccccc} e_A & n(e_A) & n(n(e_A)) & n(n(n(e_A))) & n(n(n(n(e_A)))) & \dots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \end{array} \\ &\begin{array}{cccccc} e_B & n(e_B) & n(n(e_B)) & n(n(n(e_B))) & n(n(n(n(e_B)))) & \dots \end{array} \end{aligned}$$

From here we see that N_A, N_B are almost identical, they have similar elements and the same structure.

In order to prove the main theorem let's prove at first several auxiliary lemmas.

Lemma1. a, b -are any natural numbers. **Then:** $a \neq b \Leftrightarrow n(a) \neq n(b)$ and $a = b \Leftrightarrow n(a) = n(b)$.

Proof. By definition $n: N \rightarrow N \setminus \{e\}$ is one-to-one mapping (from here immediately follows everything we need).

Def. Let a is any natural number.

Any element $n(n(\dots n(a)\dots))$ (the image of a after several mappings n) **[pict5]** is called a descendant of a .



pict.5

Lemma2. Any natural number a differs from any of it's descendants.

Proof. Let M is the set of all natural numbers, every of which differs from any of it's descendants.

Then: **[A]** $e \in M$. Really, let's assume the contrary: $e = n(n(\dots n(e)\dots))$. Then the mapping n transfers the element (natural number) $n(\dots n(e)\dots)$ into e . It is impossible, because $n: N \rightarrow N \setminus \{e\}$ and there is no any element in N that is transferred into e .

[B] if some $a \in M$, then a differs from any of it's descendants. Let's assume that $n(a) \notin M$, it means that $n(a)$ is equal to some descendant of $n(a)$, so $n(a) = n(n(\dots n[n(a)] \dots))$.

Here $n(a)$ is the element which is next to a , and on the right side we have the element $n(n(\dots n[n(a)] \dots))$ which is next to $n(\dots n[n(a)] \dots)$ and these elements are equal.

According to the **lemma1**, there must be $a = n(\dots n[n(a)] \dots)$, so a is a descendant of a , and we have a contradiction. Therefore, our assumption $n(a) \notin M$ was false, then $n(a) \in M$.

By the induction axiom $M = N$ and the **lemma2** is proved.

Lemma3. Any natural number $a \neq e$ is a descendant of one e .

Proof. Let Ω is the set of all descendants of e . Let's consider the set $M = \Omega \cup \{e\}$.

[A] $e \in M$, **[B]** If some $a \in M$, then $a \in \Omega \cup \{e\}$. If $a = e$, then $n(a) = n(e)$ and $n(a)$

is a descendant of e and $n(a) \in \Omega \Rightarrow n(a) \in M$. If $a \in \Omega$, then $a = n(n(\dots n(e) \dots))$ and $n(a) = n[n(n(\dots n(e) \dots))]$ is also a descendant of e , so $n(a) \in M$. According to the induction axiom, $M = N$, then $N = \Omega \cup \{e\}$. According to the [lemma2](#), the element e differs from any of its descendants, then e does not belong to Ω , therefore $N = \Omega \cup \{e\} \Rightarrow \Omega = N \setminus \{e\}$, then any natural number, except one, is a descendant of one.

Let's prove now the main theorem. Let N is a set of natural numbers. Let's take $e \in N$ and build the set $N_{ord} \equiv \{e, n(e), n(n(e)), n(n(n(e))), n(n(n(n(e)))) \dots\dots\dots\}$ it includes the element e and all its descendants. Let's show that N_{ord} is really a set, we have to show that there are no identical elements in the row: $\{e, n(e), n(n(e)), n(n(n(e))), n(n(n(n(e)))) \dots\dots\dots\}$ (in the other case N_{ord} contains twice the same natural number and it is not a set). Let's assume the contrary: there are some elements d, \tilde{d} in the row **[R]** $\{e, n(e), n(n(e)), n(n(n(e))), n(n(n(n(e)))) \dots\dots\dots\}$ which are equal $d = \tilde{d}$ and stay on different positions.

Without loss of generality d is on the left of \tilde{d} in **[R]**, then $N_{ord} \equiv \{e, n(e), n(n(e)) \dots d \dots \tilde{d} \dots\dots\}$. Here every element, except e , is an image of its left neighbor, then \tilde{d} is a descendant of d , so $n(\dots n(d) \dots) = \tilde{d}$. As $d = \tilde{d}$, then $n(\dots n(d) \dots) = d$ it contradicts to the [lemma2](#), therefore, there are no equal elements in **[R]**. So N_{ord} is a set, each element of N_{ord} is some natural number, then $N_{ord} \subset N$.

Conversely $N \subset N_{ord}$, really, according to the [lemma3](#), any natural number $a \neq e$ is a descendant of one, so it belongs to N_{ord} and also $e \in N_{ord}$, therefore $N \subset N_{ord}$. Then $N = N_{ord}$. The main theorem is proved.

Def. Ω is a set. And \otimes is some rule that for every pair of elements $a, b \in \Omega$ compares some element $\omega \equiv a \otimes b$ of Ω . Then \otimes is called a binary operation (or just an operation) on Ω . And we write $\otimes : \Omega \times \Omega \rightarrow \Omega$.

\otimes is called **commutative** if $a \otimes b = b \otimes a$ for any $a, b \in \Omega$.

\otimes is called **associative** if $(a \otimes b) \otimes c = a \otimes (b \otimes c)$ for any $a, b, c \in \Omega$.

Associativity means: for any $a, b, c \in \Omega$, the result of applying \otimes to the pair $(a \otimes b), c$ is always exactly the same as a result of applying \otimes to the pair $a, (b \otimes c)$.

Def. Addition "+" of natural numbers is the **binary operation** on N such that

[A] $a + e = n(a) \quad \forall a \in N$ **[B]** $a + n(b) = n(a + b) \quad \forall a, b \in N$.

Let's show that this definition is correct. There exist the unique binary operation on N with the properties **[A]** and **[B]**.

Existence. Let's take one e and define the addition " $+^e$ " on the set of all pairs $\{(e, b) \mid b \in \mathbb{N}\}$ where e is fixed and b is an arbitrary natural number. We define: $e +^e b \equiv /by\ def / \equiv n(b) \forall b \in \mathbb{N}$.

Let's check that " $+^e$ " is an addition "+" in the case $a \equiv e$.

By definition $e +^e e = n(e)$ (property **[A]**) and $e +^e n(b) = n(n(b)) = n(e +^e b)$ (property **[B]**).

Let M is the set of all natural numbers a , for every of which there exist it's own sum " $+^a$ ", which is defined on the set of all pairs $\{(a, b) \mid b \in \mathbb{N}\}$ and satisfies to **[A]** and **[B]**. By the **induction axiom** we will show that $M = \mathbb{N}$. **[A]** $e \in M$ (as were shown above) **[B]** If some $a \in M$, then it has it's own sum " $+^a$ ", which is defined on the set of all pairs $\{(a, b) \mid b \in \mathbb{N}\}$ such that **[A]** and **[B]**.

Let's take the next element $n(a)$ and define for it it's own sum " $+^{n(a)}$ " on the set of all pairs $\{(n(a), b) \mid b \in \mathbb{N}\}$ through the sum " $+^a$ ". By definition: $n(a) +^{n(a)} b \equiv /by\ def / \equiv n(a +^a b) \forall b \in \mathbb{N}$.

Then $n(a) +^{n(a)} e = n(a +^a e) = n(n(a))$ (property **[A]**) and

$n(a) +^{n(a)} n(b) = n(a +^a n(b)) = n(n(a +^a b)) = n(n(a) +^{n(a)} b)$ (property **[B]**) then $n(a) \in M$.

Therefore $M = \mathbb{N}$. It means that for every natural number a there exist it's own sum " $+^a$ ", which is defined on the set $\{(a, b) \mid b \in \mathbb{N}\}$ and satisfies **[A]** and **[B]**. Let's finally define the operation "+" on every pair (a, b) . We define: $a + b \equiv /by\ def / \equiv a +^a b$. Then "+" satisfies to **[A]** and **[B]**.

The existence is proved.

Uniqueness. Let's show that the operation "+" is unique. We assume that there exist some other addition " \oplus " with the same properties **[A]** and **[B]**. If we show that for every pair (a, b) of natural numbers $a + b = a \oplus b$, then "+" and " \oplus " are the same operation. Let's fix an arbitrary $a \in \mathbb{N}$.

Let M is the set of all natural numbers b such that $a + b = a \oplus b$. We will show that $M = \mathbb{N}$:

[A] $e \in M$, because $a + e = n(a)$ and $a \oplus e = n(a)$ (property **[A]**), then $a + e = a \oplus e$.

[B] if some $b \in M$, then $a + b = a \oplus b$, then $a + n(b) = n(a + b)$ and $a \oplus n(b) = n(a \oplus b)$

(property **[B]**) as $a + b = a \oplus b$, then according to the **lemma1**, $n(a + b) = n(a \oplus b)$, then

$a + n(b) = a \oplus n(b) \Rightarrow n(b) \in M$. Then $a + b = a \oplus b$ for any $b \in M$, but a is an arbitrary fixed natural number, therefore $a + b = a \oplus b$ for any $a, b \in M$. $a \oplus n(b) = n(a \oplus b)$

Properties of addition

Associativity. $(a + b) + c = a + (b + c)$ for any $a, b, c \in \mathbb{N}$.

Proof. Let's fix arbitrary numbers $a, b \in \mathbb{N}$. Let M is the set of all natural numbers e such that $(a + b) + c = a + (b + c)$. [A] $e \in M$, because $(a + b) + e = n(a + b) = a + n(b) = a + (b + e)$

[B] if some $c \in M$, then $(a + b) + c = a + (b + c)$. Let's consider:

$$a + b + n(c) = n((a + b) + c) = n(a + (b + c)) = a + n(b + c) = a + (b + n(c)) \Rightarrow n(c) \in M.$$

And, according to the **induction axiom**, $M = \mathbb{N}$. Then $(a + b) + c = a + (b + c)$ for any $a, b, c \in \mathbb{N}$.

Commutativity. $a + b = b + a$ for any $a, b \in \mathbb{N}$.

Step one. Commutativity for one: $a + e = e + a$ for any $a \in \mathbb{N}$.

M -is the set of all natural numbers a for which $a + e = e + a$.

[A] $e \in M$, because $e + e = e + e$ (left and right sides are exactly the same).

[B] if some $a \in M$, then $a + e = e + a$. Let's consider:

$$n(a) + e = (a + e) + e = (e + a) + e = / \text{associativity} / = e + (a + e) = e + n(a), \text{ then } n(a) \in M.$$

Therefore $M = \mathbb{N}$.

Step two. General commutativity $a + b = b + a \parallel \forall a, b \in \mathbb{N}$. Let's fix an arbitrary

natural number a . And M -is the set of all natural numbers b for which $a + b = b + a$.

[A] $e \in M$ because $a + e = e + a$ (step one).

[B] if some $b \in M$, then $a + b = b + a$. Then

$$a + n(b) = n(a + b) = n(b + a) = b + n(a) = b + (a + e) = b + (e + a) = (b + e) + a = n(b) + a \Rightarrow n(b) \in M$$

So $M = \mathbb{N}$ and commutativity is proved.

From commutativity follows that the properties [A] and [B] of addition can be rewritten as:

[A] $a + e = e + a = n(a) \quad \forall a \in \mathbb{N}$, [B] $a + n(b) = n(b) + a = n(a + b) \quad \forall a, b \in \mathbb{N}$.

Order. Let's define the order relation " $>$ " on \mathbb{N} .

Lemma4 [for order]. For any pair of natural numbers $a, b \in \mathbb{N}$ exactly one of the next cases is true:

[A] $a = b + c$ for some $c \in \mathbb{N}$ [B] $b = a + c$ for some $c \in \mathbb{N}$ [C] $a = b$.

Proof. By using the induction axiom it's very easy to prove the next auxiliary fact

Auxiliary1. There is no any natural number a , such that $a = a + b$ for some $b \in \mathbb{N}$.

From the **auxiliary1** immediately follows that: if some pair $a, b \in \mathbb{N}$ one of the cases [A],[B],[C]

is true, then any other of these cases is not true for a, b . So we can reformulate our lemma in

the equivalent form. **[Equivalent form]** For any pair of natural numbers $a, b \in \mathbb{N}$ some one of the next cases is true: [A] $a = b + c$ for some $c \in \mathbb{N}$ [B] $b = a + c$ for some $c \in \mathbb{N}$ [C] $a = b$.

Let's fix an arbitrary $a \in \mathbb{N}$. Let M is the set of all natural b , for every of which some one of the cases [A],[B],[C] is true.

[A] $b \equiv e \in M$. Really, if $a = e$, then the case [C] is true. Let $a \neq e$, then,

according to the [lemma3](#), a is a descendant of e , so

$$\begin{aligned} a &= n(\dots n(n(n(e)))\dots) = // n(e) = e + e // = n(\dots n(n(e + e))\dots) = // n(e + e) = (e + e) + e // = \\ &= n(\dots n((e + e) + e)\dots) = // n((e + e) + e) = ((e + e) + e) + e // = \dots = (e + (e + \dots (e + e))) + e \equiv c + e = e + c, \\ \text{then } a &= e + c, \text{ and we have the case [A]. So } e \in M. \end{aligned}$$

[B] if some $b \in M$, then [A] $a = b + c$ or [B] $b = a + c$ or [C] $a = b$. Let's consider $n(b) = b + e$.

Let we have [A] $a = b + c$. If $c = e$, then $a = b + e = n(b)$, then we have the case [C] for the pair $a, n(b)$. If $c \neq e$, then (as we showed above) $c = e + \Delta$ where $\Delta \in \mathbb{N}$, then

$$a = b + c \Leftrightarrow a = b + (e + \Delta) = / \text{associativity} / = (b + e) + \Delta = n(b) + \Delta, \text{ then we have the case [A]}$$

for the pair $a, n(b)$. Let we have [B] $b = a + c$, then

$$n(b) = b + e = (a + c) + e \Rightarrow n(b) = a + (c + e) \Leftrightarrow n(b) = a + n(c), \text{ so we have the case [B] for}$$

the pair $a, n(b)$. Let we have [C] $a = b$, then $n(b) = b + e = a + e \Rightarrow n(b) = a + e$ so we have the case [B] for the pair $a, n(b)$. So, in any case: if $b \in M$, then $n(b) \in M$, therefore,

by the induction axiom, $M = \mathbb{N}$. Everything is proved.

Def. Let $a, b \in \mathbb{N}$ are any natural numbers. In the case [A] $a = b + c$ we will write $a > b$.

In the case [B] $b = a + c$ we will write $b > a$.

[Assertion1](#). " $>$ " is an order relation on \mathbb{N} (and \mathbb{N} is an ordered set).

Proof. Put simply, we need to show that any elements $a, b \in \mathbb{N}$ are comparable, and that " $>$ " is transitive, then (by definition) " $>$ " is an order relation on \mathbb{N} . From the [lemma4](#) follows that for any elements $a, b \in \mathbb{N}$ only one of the next cases is true: $a = b$, or $a < b$, or $b < a$.

And the relation " $>$ " is transitive: let $a < b$ and $b < c$, then $a + \Delta = b$ and $b + \delta = c$, then $(a + \Delta) + \delta = b + \delta \Rightarrow a + (\Delta + \delta) = b + \delta \Rightarrow a + (\Delta + \delta) = c \Rightarrow a < c$.

During the proof of the [lemma4](#) we have shown that if $a \neq e$, then $a = e + c$, so any natural number $a \neq e$ is greater than e . Therefore, e is the least natural number. And for any natural a obviously $a < n(a)$. And numbers $a, n(a)$ are neighbors (there is no any natural b such that $a < b < n(a)$).

Really, if $a < b < n(a)$, then $a < b$, then $a + \Delta = b$. As $b < n(a) \Rightarrow a + \Delta < n(a)$. If $\Delta = e$, then we have $a + e < n(a) \Rightarrow n(a) < n(a)$, therefore $\Delta \neq e$. As $\Delta \neq e$, then, as we showed above, there must be $\Delta = e + \omega$, then $a + \Delta < n(a) \Rightarrow a + (e + \omega) < n(a) \Rightarrow (a + e) + \omega < n(a) \Rightarrow n(a) + \omega < n(a)$ and we have a contradiction, because $n(a) + \omega > n(a)$. So, finally, there is no any b such that $a < b < n(a)$ and $a, n(a)$ are neighbors.

Def. $(\Omega, <)$ is some ordered set. Elements $a, c \in \Omega$ are called **neighbors** if there is no any $b \in \Omega$, such that $a < b < c$, or $c < b < a$. The element $a \in \Omega$ is called **the first** if $a < b$ for any other $b \in \Omega$. The element $a \in \Omega$ is called **the last** if $b < a$ for any other $b \in \Omega$.

Obviously e is the first natural number. And there is no last number in \mathbb{N} .

Subtraction "-"

Def. Let's consider the set Ω of all pairs (a, b) where $a > b$. Subtraction "-" is the mapping $\Omega \rightarrow \mathbb{N}$, which for every pair $(a, b) \in \Omega$ compares the natural number c such that $a = b + c$. We will denote $c \equiv a - b$, and we will say that c is a "difference of a and b ".

So, by definition, for any $a > b$ we have $a = b + (a - b)$. Addition "+" is commutative, therefore we can write $b + (a - b) = (a - b) + b = a$ for any $a > b$.

Assertion2. For any $a > b$, the difference $a - b$ is uniquely defined.

Proof. Let's notice that if $c > \Delta$, then $b + c > b + \Delta$. Really, $c > \Delta \Rightarrow c = \Delta + \omega$, then $b + c = b + (\Delta + \omega) = (b + \Delta) + \omega > b + \Delta$. Let's assume that $a - b = c$ and $a - b = \Delta$, then, according to the definition of "-", there must be $a = b + c$ and $a = b + \Delta$, then $b + c = b + \Delta$. If $c < \Delta$, then $b + c < b + \Delta$, if $c > \Delta$, then $b + c > b + \Delta$. Therefore $c = \Delta$.

Exercise. For any $a, b, c, d \in \mathbb{N}$ (where $a > b$ and $c > d$) the next formulas are true:

- [A]** $a > a - b$, **[B]** $a - b = c - d \Leftrightarrow a + d = b + c$, **[C]** $(a - b) + (c - d) = (a + c) - (b + d)$,
- [D]** $(a - b) - (c - d) = (a + d) - (b + c)$ (in this property there is a requirement $(a - b) > (c - d)$),
- [E]** $a = b \Leftrightarrow m - a = m - b$ (for any $m > a, m > b$) $\Leftrightarrow a - c = b - c$ (for any $c < a, c < b$),
- [F]** $a > b \Leftrightarrow m - a < m - b$ (for any $m > a, m > b$) $\Leftrightarrow a - c > b - c$ (for any $c < a, c < b$).

Def. Let Ω is an ordered set and X is a subset of Ω . The element $M_{\max} \in X$ is called the greatest element of X if for any $x \in X: x \leq M_{\max}$. The element $m_{\min} \in X$ is called the least element of X if for any $x \in X: x \geq m_{\min}$.

Theorem1. Any nonempty subset $X \subset \mathbb{N}$ of natural numbers has the least number m_{\min} .

If there exist some number M such that $x < M \parallel \forall x \in X$, then X also has the greatest number M_{\max} .

Proof. Let's fix an arbitrary subset X of natural numbers. If $e \in X$, then e is the least number of X . Let $e \notin X$. Let's consider the set $L = \{a \parallel a < x, \forall x \in X\}$, obviously $e \in L$. There exist some natural number Δ such that $\Delta \in L$, but $n(\Delta) \notin L$ (if there is no such number, then, by the **induction axiom**, $L = \mathbb{N}$ and X is empty).

Let's show that $n(\Delta)$ is the least number in L .

[A] Let's show that $n(\Delta) \in X$. We consider the set $G = \{a \parallel a > x, \forall x \in X\}$. Then the set of natural numbers \mathbb{N} is divided into the sets L, X, G and these sets do not have any common elements. We know that $n(\Delta) \notin L$, then $n(\Delta) \in X$, or $n(\Delta) \in G$.

If G is an empty set, then $n(\Delta) \in X$, and we go to the step [B].

If G is not an empty set and $n(\Delta) \in G$, then: Δ is less than any number of X and $n(\Delta)$ is greater than any number of X . Then there exist some $\tilde{x} \in X$ such that $\Delta < \tilde{x} < n(\Delta)$ which is impossible, because $\Delta, n(\Delta)$ are neighbors. So, in any case $n(\Delta) \notin G$, then there must be $n(\Delta) \in X$.

[B] Let's show that $n(\Delta) \leq x$ for any $x \in X$. If it's not true, then there exist some $\tilde{x} \in X$ such that $\tilde{x} < n(\Delta)$. As Δ is less than any number of X , then again $\Delta < \tilde{x} < n(\Delta)$, which is impossible.

Therefore $n(\Delta) \leq x, \forall x \in X$. From [A] and [B] follows that $n(\Delta)$ is the least number of X .

Let there exist some natural number M such that $x < M \parallel \forall x \in X$.

Let's consider again the set $G = \{a \parallel a > x, \forall x \in X\}$ - this set is not empty, because it contains M .

Then G has the least number g_{\min} . Obviously $g_{\min} \neq e$ (really, if $g_{\min} = e$, then X must be empty).

As $g_{\min} \neq e$, then $g_{\min} > e$ and $n(g_{\min} - e) = g_{\min}$.

[C] Let's show that $(g_{\min} - e) \in X$. As we have shown above, the set N is divided into the sets L, X, G without common elements. For sure $(g_{\min} - e) \notin G$ (because if $(g_{\min} - e) \in G$, then g_{\min} is not the least number in G). If L is an empty set, then $(g_{\min} - e) \in X$ and we go to the step [D].

Let L is not empty, let's assume that $(g_{\min} - e) \in L$. Then for every $x \in X$ there must be $(g_{\min} - e) < x < g_{\min}$ which is impossible, because $(g_{\min} - e)$ and g_{\min} are neighbors.

Therefore, in any case $(g_{\min} - e) \notin L \Rightarrow (g_{\min} - e) \in X$.

[D] Let's show that $(g_{\min} - e) \geq x$ for any $x \in X$. If it is not true, then there exist $\tilde{x} \in X$ such that $(g_{\min} - e) < \tilde{x}$. Then $(g_{\min} - e) < \tilde{x} < g_{\min}$ which is impossible, because $(g_{\min} - e)$ and g_{\min} are neighbors. Then $(g_{\min} - e) \geq x$ for any $x \in X$. From [C] and [D] follows that $(g_{\min} - e)$ is the greatest number of X .

Any set of natural numbers can be written as

$N \equiv \{e, n(e), n(n(e)), n(n(n(e))), n(n(n(n(e)))) \dots\}$, this writing is very voluminous, that's why we denote: $e \equiv 1, n(e) \equiv 2, n(n(e)) \equiv 3, \dots, n(n(n(n(n(n(n(n(n(e)))))))) \equiv 10$.

Then $N \equiv \{1, 2, 3, \dots, 10, n(n(n(n(n(n(n(n(n(1)))))))) \dots\}$ [N]. We will show later

the possibility of a decimal notation: any natural number can be written in a unique way as a combination of symbols 0,1,2...9. Now we do not have sufficient instruments to prove it.

For example, we do not have a zero number 0 in N , this number will appear only when we build the ring of integer numbers. We could add the zero number now, but then we would have to go through all the previous theory and check that all the properties and assertions are still true for the new set $N \cup \{0\}$. Such approach is very inconvenient. Also, the proof of the possibility of a decimal notation requires some facts from the divisibility theory, and this theory can be build for integer numbers. That's why we will use the notation [N] of natural numbers for a while.

[Ordinary induction]. T is any assertion which makes a claim that is based on k , where k is some natural number. If $[step\ A]$ and $[step\ B]$ are true, then T is true for every natural number k

$[step\ A]$ T is true in the case when $k = 1$,

$[step\ B]$ If T is true for some number k , then T **must be** true for the next number $n(k)$.

Proof. T is our assertion and both $[step\ A]$ and $[step\ B]$ are true.

Let's denote the set $M = \{all\ natural\ numbers\ k, \text{ for which } T \text{ is true}\}$. Let's show that $M = N$, by using the induction axiom. From here will follow that T is true for every natural number k .

$1 \in M$ because of the $[step\ A]$. If some natural number k belongs to M , then T is true for this number k . Because of the $[step\ B]$, the assertion T must be true for the next natural number $n(k)$ and therefore $n(k) \in M$. Then: if some $k \in M$, then $n(k) \in M$.

According to the **induction axiom**, $M = N$.

Def. For any natural number k , the set $\{a \in N \mid 1 \leq a \leq k\}$ is called a segment of natural numbers, and we denote it like $[1, k]$.

The set of natural numbers can be written as

$N \equiv \{1, 2, 3, \dots, 10, n(n(n(n(n(n(n(n(n(1)))))))))) \dots\} [N]$. From $[N]$ follows that all the numbers of any segment $[1, k]$ go one after another in $[N]$, starting from 1 and up to k .

And therefore, we can agree to use the similar notation for any segment $[1, k]$. So,
 $[1, 1] = \{1\}$, $[1, 2] = \{1, 2\}$, $[1, 3] = \{1, 2, 3\}$... $[1, 8] = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

Segments $[1, k]$ and $[1, m]$ are equal (equal as sets) $\Leftrightarrow k = m$.

Reminder: set's A and B are called equivalent $A \approx B$ if there exist one-to-one mapping $f : A \rightarrow B$

Def. A is a set of any kind. If there exist some segment of natural numbers $[1, k]$ such that $A \approx [1, k]$, then we say " A is a finite set" and "there are k elements in A ".
 And we write $|A| = k$.

Assertion1. The given definition is correct. If some set A is equivalent to some segment of natural numbers, then that segment is unique (there can't be $A \approx [1, k]$ and $A \approx [1, m]$, where $[1, k] \neq [1, m]$).

Assertion T (auxiliary). For any $k \in N$: if $[1, k] \neq [1, m]$, then $[1, k]$ is not equivalent to $[1, m]$.

Proof. By **ordinary induction**. $[step\ A]$ " T is true in the case when $k = 1$ ".

We have to show: if $[1, 1] \neq [1, m]$, then these segments are not equivalent. As $[1, 1] \neq [1, m]$, then $m \neq 1$, then $m > 1$, then the set $[1, m]$ contains 1 and 2 (and maybe some other numbers).

Let's assume that the segments are equivalent, then $[1, 1] \approx [1, m]$, then there exist one-to-one mapping $f : [1, 1] \rightarrow [1, m] \Leftrightarrow f : \{1\} \rightarrow [1, m]$. If $f(1) = 1$, then 2 does not have any pre-image in $\{1\}$.

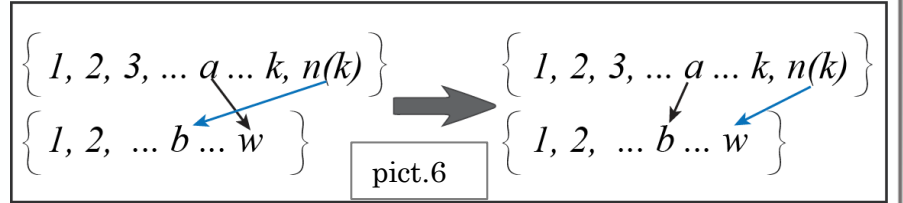
If $f(1) = 2$, then 1 does not have any pre-image in $\{1\}$. If $f(1) \neq 1$ and $f(1) \neq 2$, then both 1 and 2 do not have any pre-image in $\{1\}$. Therefore f is **not** one-to-one, and we have a contradiction. So, T is true when $k = 1$.

[step B] if T is true for some natural number k . So, for $[1, k]$ we have: if $[1, k] \neq [1, m]$, then these segments are not equivalent. We have to show that the same is true for $n(k)$.

Let's assume the contrary: $[1, n(k)] \neq [1, w]$, but these segments are equivalent. Then there exist one-to-one mapping $f : [1, n(k)] \rightarrow [1, w]$. Here $w > 1$. Really, if $w = 1$, then $[1, n(k)] \approx [1, 1]$ which is impossible, because $n(k) > 1 \Rightarrow [1, n(k)] \neq [1, 1]$, then these segments can't be equivalent ([step A]).

So $w > 1$.

$f : [1, n(k)] \rightarrow [1, w]$ is one-to-one mapping. Then for some $a \in [1, n(k)] \Rightarrow f(a) = w$ and for some $b \in [1, w] \Rightarrow f(n(k)) = b$ [pict6].



Then we will slightly redefine f : [earlier] $f(a) = w$ and $f(n(k)) = b$ [and now] $f(a) \equiv b$ and $f(n(k)) \equiv w$. And f is still the same on any other element of the set $[1, n(k)]$. So f is still one-to-one mapping $f : [1, n(k)] \rightarrow [1, w]$, but now it maps the end of the segment into the end of the segment: $f(n(k)) \equiv w$. Then we can discard the elements $n(k), w$ from $[1, n(k)]$, $[1, w]$ and f still will be one-to-one mapping $f : [1, k] \rightarrow [1, (w-1)]$. Let's notice that $[1, k] \neq [1, (w-1)]$. Really, if $[1, k] = [1, (w-1)]$, then $[1, n(k)] = [1, w]$, but we have assumed that $[1, n(k)] \neq [1, w]$. Then $[1, k] \neq [1, (w-1)]$ and there is one-to-one mapping $f : [1, k] \rightarrow [1, (w-1)]$, it contradicts to our initial assumption (at the beginning of the [step B]). Therefore, if $[1, n(k)] \neq [1, w]$, then these segments are not equivalent. And T is true for $n(k)$.

The steps [step A] and [step B] of the **ordinary induction** are completed.

Then the **assertion** T is true for every natural number k .

Let's prove now the **assertion1**. We assume the contrary: $A \approx [1, k]$ and $A \approx [1, m]$ where $[1, k] \neq [1, m]$. Then, by transitivity, $[1, k] \approx [1, m]$ and $[1, k] \neq [1, m]$ which is impossible, according to the **assertion** T . Therefore, if $A \approx [1, k]$, then the segment $[1, k]$ is unique, there is no any other segment of natural numbers that is also equivalent to $[1, k]$. Everything is proved.

Def. A is a set of any kind. If A is an empty set, then it is a finite set by **definition**.

If A is not an empty set and A is not equivalent to any segment $[1, k]$, then we say “ A is an infinite set” or “there are infinitely many elements in A ”.

According to the previous definition, any set A is either finite or infinite and no other variants.

Assertion2. A is a finite set and $|A| = k > 1$. Then for any $a \in A$ we have $|A \setminus \{a\}| = (k - 1)$.

Proof. As $|A| = k$ there exist one-to-one mapping $f : A \rightarrow [1, k]$.

Let's fix some $a \in A$, if $f(a) = k$, then we discard the elements a, k from $A, [1, k]$, and f will become one-to-one mapping $f : A \setminus \{a\} \rightarrow [1, (k - 1)]$, then $|A \setminus \{a\}| = (k - 1)$.

If $f(a) \neq k$, then we can slightly redefine f (as we did above) such that $f(a) = k$, and we will get again $|A \setminus \{a\}| = (k - 1)$.

Assertion3. A is a finite set, then any subset $B \subset A \parallel B \neq A$ is also a finite set and $|B| < |A|$.

Proof. Let $|A| = k$, we can reformulate our assertion:

(**Assertion** \tilde{T}) $|A| = k$, then for any $B \subset A \parallel B \neq A$ there must be $|B| < k$. We prove it by induction.

[step A] Let $k = 1$, then $|A| = 1$. Then there is only one element a in A , so $A = \{a\}$.

If $B \subset A \parallel B \neq A$, then $B = \emptyset$. Then B is a finite set (by definition). And \tilde{T} is true when $k = 1$.

[step B] Let \tilde{T} is true for some natural number k , i.e., if $|A| = k$, then for any $B \subset A \parallel B \neq A$ we

have $|B| < k$. Let's consider the case $|A| = n(k)$. According to the **assertion2**, for any element $a \in A$ there must be $|A \setminus \{a\}| = k$. Let's fix now any subset $B \subset A \parallel B \neq A$. As $B \neq A$ there exist the element $a \in A$ such that $a \notin B$. Then $B \subset A \setminus \{a\}$.

If $B = A \setminus \{a\}$, then $|B| = |A \setminus \{a\}| = k < n(k) \Rightarrow |B| < n(k)$.

If $B \neq A \setminus \{a\}$ (and $B \subset A \setminus \{a\}$), then, according to our assumption, (at the beginning of the [step B])

there must be $|B| < |A \setminus \{a\}| = k < n(k) \Rightarrow |B| < n(k)$. So the steps [step A] and [step B] are

completed, then our assertion \tilde{T} is true for every natural number

k . And the **assertion3** is proved.

Consequence1. A is a set. If there exist some subset $B \subset A \parallel B \approx A, B \neq A$ [pict7], then A is an infinite set.

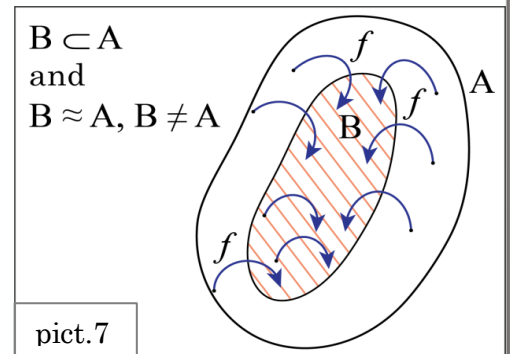
Proof. Let's assume the contrary: A is a finite set.

Let's notice that $A \neq \emptyset$. Really, if $A = \emptyset$, then $B \subset A \Rightarrow B = \emptyset$ and therefore $B = A$, which contradicts to the requirement

$B \neq A$. Then there exist some segment $[1, k]$ such that $A \approx [1, k]$. As $B \approx A$, then $B \approx [1, k]$, then

$|B| = |A| = k$. We also have $B \subset A \parallel B \neq A$, then (**assertion2**) $|B| < |A|$, but $|B| = |A| = k$ and we have a contradiction. Therefore A is an infinite set.

Consequence2. The set of natural numbers \mathbb{N} is an infinite set.



Proof. $n: \mathbb{N} \rightarrow \mathbb{N} \setminus \{e\}$ is one-to-one mapping. And the set \mathbb{N} is equivalent to its subset $\mathbb{N} \setminus \{e\}$. According to the [consequence1](#), \mathbb{N} is an infinite set.

[Advanced induction]. T is any assertion which makes a claim that is based on k , where k is some natural number. If $[step\ A]$ and $[step\ B]$ are true, then T is true for every natural number k

$[step\ A]$ T is true in the case when $k = 1$,

$[step\ B]$ If T is true for some natural numbers $1, 2 \dots k$, then T **must be** true for the number $n(k)$.

Proof. T is our assertion and both $[step\ A]$ and $[step\ B]$ are true.

Let X is the set of all natural numbers k , for which T is **not true**. If X is an empty set, then T is true for every natural number k . Let $X \neq \emptyset$, then according to the [theorem1](#), the set X has the least number $x_{\min} \in X$. Notice that $x_{\min} \neq 1$ (really, if $x_{\min} = 1$, then T is not true for the number 1, but according to the $[step\ A]$, the [assertion](#) T is true for 1).

So x_{\min} is a minimal number for which T is not true. Then T is true for any natural number $a < x_{\min}$. So T is true for $1, 2 \dots (x_{\min} - 1)$, then, according to the $[step\ B]$, the [assertion](#) T must be true for the number $n(x_{\min} - 1) = x_{\min}$, then $x_{\min} \notin X$, and we have a contradiction. Therefore $X = \emptyset$, and T is true for every natural number k .

The rules of calculation of an expression with some arrangement of brackets.

"+": $A \times A \rightarrow A$ is any binary operation (for any elements $a, b \in A$ it compares some element $a + b$ of A). We will call it an "addition". Everywhere later $a, b, c, d, e \dots m$ are any elements of A .

Quite often we have to consider sums of elements of A . For example, the expression $(a + b) + (c + d)$ denotes the sum of elements $(a + b)$ and $(c + d)$, the expression $(a + b + c) + d$ denotes the sum of elements $(a + b + c)$ and d . Are these sums equal? The answer is yes, **if** the operation "+" is associative. We will show it soon. Let's define the basic rules, according to which we must calculate any expression.

Σ Def . Any sum $a + b + c + d + \dots + m$ without any brackets must be calculated in the next way: we take a and add b to it from the right side, then we get $(a + b)$, then we add c to it from the right side. Then we get $((a + b) + c)$, then we add d to it from the right side. Then we get $((a + b) + c) + d$ and etc. In the end we will have the element $\dots(((a + b) + c) + d) + \dots + m$, by definition, this element is equal to the sum $a + b + c + d + \dots + m$.

So $a + b + c + \dots + m \equiv /by\ def/ \equiv \dots(((a + b) + c) + d) + \dots + m$ - this arrangement of brackets is called the **standard arrangement** of brackets. We say that brackets are arranged here in the **standard way**.

When there is only one element a in the sum, the standard arrangement of brackets has no brackets at all. Even for the sum $a + b$ there are no brackets at all in the standard arrangement. Only when we have the sum like: $a + b + c$, then the standard arrangement of brackets is $(a + b) + c$. And for any sum $a + b + c + d$, the standard arrangement is $((a + b) + c) + d$ and etc.

In general a sum of several elements with some arrangement of brackets is called an “expression”. The “expression” is some collection of summands a, b, c, d, \dots , signs “+” and pairs of brackets $[], (), \{ \}$. Summands a, b, c, d, \dots are always elements of some fixed set A , where the operation “+” is defined.

Pairs of brackets must be arranged reasonably. Any pairs $[], ()$ may be arranged only like this $.....$.. or like this $(...[...])$.. The arrangement like $..[...(...)]$.. is forbidden.

If some brackets $[]$ contain only one element d , then we can discard these brackets: $[d] \rightarrow d$. And similarly, if some brackets $[]$ contain the whole initial expression, we can also discard them. If some brackets $[]$ contain some other brackets $()$ inside and there are no elements between them $[()]$, then we can discard the internal brackets: $[()] \rightarrow []$.

Example. The next arrangements of brackets is admissible: $a + (b + c + \{d + e + [....]... \}....).... + m$. Any summands a and b of any expression must be considered as different elements. And therefore, every summand in any expression is unique, and we can speak about a **set of all summands** (of any expression). Similarly, we can speak about a **set of all pairs of brackets** $[], (), \{ \}$ (of any expression).

The main restriction. From now on we consider only such expressions, in which a set of all summands and a set of all pairs of brackets are **both** finite sets. Moreover, we consider only expressions with admissible arrangements of brackets that do not have any redundant brackets that can be discarded.

If the set of all summands (of some expression) is equivalent to some segment $[1, k]$ of natural numbers, we say that “the expression contains k elements” or “the expression consists of k elements” (or “there are k elements in the expression”) or just that “we have a **finite expression**”.

Any expression denotes a sum of several elements of A , which must be calculated in a certain way (the process is described in the [Step 1 \Rightarrow] and [Step 2 \Rightarrow] below). In any case, for any expression, the result of our calculations is always some element $v \in A$.

[Step 1 \Rightarrow] In order to calculate an expression with some arrangement of brackets we always “move” from the leftmost element to the right. We will go through some elements and left brackets $a + (b + c + \{d + e + [..$ until we meet **any** right bracket on our way: $], \},)$.

For example, we met a square bracket $]$, it means that we have already passed $[$. And now we are exactly between these square-brackets $[... here ...]$ (notice that there is no any other pair of brackets $\{ \}$ inside $[]$, because $]$ is the first right bracket on our way).

Now we need to calculate the expression [expression] in these brackets, by using the Σ Def from above, the result is some element S . Then all the internal expression [expression], together with it's outer brackets [...] must be replaced by S , so [...] $\xrightarrow{\text{replaced by}} S$.

[Step 2 \Rightarrow] Now we have the new expression $a + (b + c + \{d + e + S\} \dots) \dots + m$.

We have to return to it's leftmost element. And we do exactly the same thing that we described in the [Step 1 \Rightarrow] (we move from the leftmost element to the right until we meet any right bracket } on our way). Every time when we complete the [Step 1 \Rightarrow] we discard one element from the set of pairs of brackets. The set Ω of all pairs brackets is a finite set, let it contains $n = |\Omega|$ elements.

Then after n performances of the [Step 1 \Rightarrow] we will get "the final" expression without any brackets at all. If the initial expression contained k elements, then the final expression (for sure) contains $t \leq k$ elements. If the final expression consists of one element, then that element must be taken as a result of our calculations. If the final expression consists of several elements, then their sum must be calculated according to the Σ Def, and the result must be taken as a result of our calculations. So, in the result we will always get some element $v \in A$, then, by definition, our initial expression is equal to v .

Def. Let we have some expression $a + (b + c + \{d + e + [\dots] \dots\} \dots) \dots + m$ with some arrangement of brackets. When we make actions like [A] and [B] we say that we "rearrange brackets in the expression".

[A] We discard any pairs of brackets from our expression.

[B] We place some new pairs of brackets in our expression (after [A] or before [A]).

And we say that we make the standard rearrangement of brackets if we discard all the brackets from the expression and we place the new brackets in the standard way:

$$(\dots(((a + b) + c) + d) + \dots) + m.$$

If "+" : $A \times A \rightarrow A$ is an associative operation. Then we can rearrange brackets in any expression in any way we want, a new expression will be always equal to an initial expression. This assertion follows from the [main theorem2](#), but at first, let's consider the next example.

Let's look at the expression $(a + b) + (c + d)$, we can consider $(a + b)$ as a sum of elements a and b and the sum $(c + d)$ as a separate element, then, by associativity:

$$(a + b) + (c + d) = a + (b + (c + d)). \text{ Now we can apply the associative law to the sum } b + (c + d) = (b + c) + d, \text{ then } (a + b) + (c + d) = a + ((b + c) + d).$$

We can consider the last expression as a sum of elements a , $(b + c)$, d . Then, by associativity:

$$(a + b) + (c + d) = (a + (b + c)) + d. \text{ We have deduced that the expressions } (a + b) + (c + d) \text{ and } (a + (b + c)) + d \text{ are equal, despite the fact that they have different arrangements of brackets.}$$

Assertion4. Let we have an expression with k elements with some arrangement of brackets, then any brackets $\{ \}$ which do not contain the whole expression, contain an expression with $m < k$ elements. The proof is obvious here.

The main theorem2 (the main property of any associative operation).

A is a set. And $"+" : A \times A \rightarrow A$ is any binary **associative** operation on A .

Then: Any finite expression (which consists of k elements) will not change after the standard rearrangement of brackets.

Proof. Let's use an **advanced induction**. [step A] T is obviously true in the case when $k = 1$.

In such case an expression consists of only one element a and there are no any brackets.

(There can't be brackets (a) or $[(a)]$, because we have agreed not to consider expressions that have any redundant brackets). And the standard arrangement of brackets for the expression a also has no brackets at all, so we already have the standard arrangement.

[step B] if T is true for some numbers $1, 2 \dots k$. Then any expression with $1, 2 \dots k$ elements will not change after the standard rearrangement of brackets.

Let's take an arbitrary expression with $n(k)$ elements, let $a_{n(k)}$ is it's last summand.

[First case] If there are no brackets on the right of $a_{n(k)}$, then our expression is:

the expression on the left of $a_{n(k)} + a_{n(k)}$.

[A] If the whole expression on the left of $a_{n(k)}$ is already captured by some brackets, then the whole expression is the sum: [the expression on the left of $a_{n(k)}$] $+ a_{n(k)}$. The expression on the left of $a_{n(k)}$ consists of k elements, therefore, it will not change if we rearrange brackets in it in the standard way, then the initial expression is equal to $[(\dots(((a + b) + c) + d) + \dots) + m] + a_{n(k)}$ -here we have the standard arrangement.

[B] If the expression on the left of $a_{n(k)}$ is not captured by any brackets, then there can be the next cases:

[1-st case] The expression on the left of $a_{n(k)}$ consists of one element b , then b can't be captured by any brackets, so the total expression is $b + a_{n(k)}$ and there are no any brackets in the standard arrangement for such sum and we already have the standard arrangement.

[2-nd case] The expression on the left of $a_{n(k)}$ consists of more than one element.

Then, according to **the rules of calculation of an expression with brackets** ([Step 1 \Rightarrow] and

[Step 2 \Rightarrow]), the expression on the left of $a_{n(k)}$ must be calculated at first in any case, regardless of the arrangement of brackets in this expression.

Then we can enclose this expression in the new brackets, because in any case it must be calculated at first, so: the expression on the left of $a_{n(k)} + a_{n(k)} = [\text{the expression on the left of } a_{n(k)}] + a_{n(k)}$.

And again, the expression inside the square brackets consists of k elements and therefore it will not change if we rearrange brackets in it in the standard way. Then our initial expression is equal to $[(...(((a+b)+c)+d)+...) + m] + a_{n(k)}$ -here we have the standard arrangement.

[Second case] Let there is one or several brackets $],),\}$ on the right of $a_{n(k)}$.

Let's take the rightmost bracket $\}$. The brackets $\{\}$ can't contain the whole expression (if $\{\}$ contain the whole expression, then these are redundant brackets). Then the initial expression is a sum of two expressions: the expression which stays on the left of $\{\}$ and the expression which stays inside $\{\}$. According to the [assertion4](#), the expression inside $\{\}$ consists of $m < n(k)$ elements. And similarly, the expression on the left of $\{\}$ consists of $h < n(k)$ elements. Then, according to our assumption, (at the beginning of the [step B]) we can rearrange brackets in each of these expressions in the standard way, each of these expressions will not change.

Then the initial expression is a sum of two expressions with standard arrangements of brackets:

$$(...(((a+b)+c)+...) + v) + \{ (...(((q+w)+x)+...+u) + a_{n(k)} \} \equiv (S) + \{ (\tilde{S}) + a_{n(k)} \} =$$

$$= / \text{associativity} / = ((S) + (\tilde{S})) + a_{n(k)}.$$

The expression $((S) + (\tilde{S}))$ consists of k elements and (according to our assumption) it will not change if we rearrange brackets in it in the standard way:

$$((S) + (\tilde{S})) = (...(((a+b)+c)+...) + ...) + ... + u.$$

Then the initial expression is equal to

$$(...(((a+b)+c)+...) + ...) + ... + u + a_{n(k)}$$

-here we have the standard arrangement of brackets.

So the [step A] and [step B] (of induction) are completed. Therefore, our [assertion T](#) is true for any expression with k elements. Everything is proved.

Conclusion. From [the main theorem2](#) follows that: if the operation $+$: $A \times A \rightarrow A$ is associative, then in any given expression we can rearrange brackets in any way we want (we can choose the arrangement of brackets which is more convenient for calculations). A new expression is always equal to an initial expression.

Def. Let we have some finite expression with some arrangement of brackets. And a, b are some summands. We replace a by b and b by a , and we do not change any other summands, or signs $+$, or brackets $[], (), \{\}$. Then we say that “we permute elements a, b ”.

Assertion5. If the operation $+$: $A \times A \rightarrow A$ is not only associative, but also commutative, then any finite expression will not change after permutation of any of it's elements.

Lemma5. If $+$: $A \times A \rightarrow A$ is associative and commutative, then in any expression we can permute elements which stay near by, an expression will not change.

Proof. Let's take any expression and remember the initial arrangement of brackets in it, we will change it for a while, but then we will return back to it. Let's assume that the elements a, b which we want to permute, are neighbors, so we can place them in the round brackets $()$. All the elements

which are on the left of a and b (if there are such elements) we place in the square brackets $[]$, and all the elements which are on the right of a and b (if there are such elements) we place in $\{\}$.

Then:

The initial expression $= [c + d + \dots + m] + (a + b) + \{h + u + \dots + x\} = // \text{commutativity } a + b = b + a // = [c + d + \dots + m] + (b + a) + \{h + u + \dots + x\} = // \text{Let's return the initial arrangement of brackets} // = \text{The expression we need.}$ The last expression is exactly the initial expression, where a and b are permuted.

Let's prove now the [assertion5](#). Let we have some expression where we need to permute some elements a, b . If these elements stay near by, then, by [lemma5](#), we can permute them and the expression will not change.

Let elements a, b are not near by. Without loss of generality a is on the left of b .

Then we can permute a with it's "right neighbors" until a and b become neighbors.

Then we permute a and b . Then we permute b with it's "left neighbors" until b stays on the initial position of a . So, by making several permutations of elements that stood near by, we have permuted a and b . Notice that during these permutations we haven't changed any brackets, or signs "+" in our expression, we just permuted some neighbor elements. Now we have the "final expression" which is exactly what we need. Any permutation of neighbor elements gives an equal expression ([lemma5](#)). Then initial and final expressions are equal. Everything is proved.

Conclusion. If "+" : $A \times A \rightarrow A$ is associative and commutative, then in any expression we can rearrange brackets in any way we want, and we can permute elements how we want, it will not change an expression.

We have already proved that the addition "+" of natural numbers is commutative and associative, therefore, in any sum of natural numbers with any arrangement of brackets we can rearrange brackets how we want and permute numbers how we want, a sum will not change.

Therefore, if we have sums of natural numbers and these sums consist of the same numbers, then these sums are equal.

For example: $((a + b) + c) + d + (e + m) = b + (c + a) + (m + d) + e$ for any natural numbers a, b, c, d, e, m .

Reminder. Ordered sets $(A, <)$ and $(B, \tilde{<})$ are called isomorphic if there exist one-to-one $f : A \rightarrow B$ such that $a < b$ (in A) $\Leftrightarrow f(a) \tilde{<} f(b)$ (in B).

Theorem3. Any sets N_A and N_B of natural numbers are isomorphic (isomorphic as ordered sets).

Proof. Let N_A and N_B are our sets. We define $1_A \xrightarrow{f} 1_B$ and if $a_A \xrightarrow{f} a_B$, then $n(a_A) \xrightarrow{f} n(a_B)$. In other words, by definition: $f(1_A) \equiv 1_B$ and if $f(a_A) = a_B$, then $f(n(a_A)) \equiv n(a_B)$. We can see that f is a rule that for some elements of N_A compares some elements of N_B .

[Step1] Let's show that f is defined on all N_A , we need to show that for every $a_A \in N$ the element $f(a_A)$ exists, and it is some element of N_B .

Let M_A is the set of all elements a_A of N_A , for every of which the element $f(a_A)$ exists.

[A] $1_A \in M_A$ because $f(1_A) = 1_B$, [B] if some $a_A \in M_A$, then $f(a_A) = a_B$ for some $a_B \in N_B$, from the equality $f(a_A) = a_B$ and the definition of f follows that $f(n(a_A)) = n(a_B)$, so for $n(a_A)$ the element $f(n(a_A))$ does exist. Then $n(a_A) \in M_A$. And $M_A = N_A$. And now we can say that f is a mapping from N_A to N_B .

[Step2] Let's show that f fully covers N_B . Let M_B is a subset of N_B , the set M_B consists of all elements a_B which have some pre-image in N_A . [A] $1_B \in M_B$, because $f(1_A) = 1_B$.

[B] if some $a_B \in M_B$, then $f(a_A) = a_B$ for some $a_A \in M_A$, from here (according to the definition of f) immediately follows that $f(n(a_A)) = n(a_B)$, and it means that $n(a_B) \in M_B$. So $M_B = N_B$, then f fully covers N_B .

[Step3] Let's show that f doesn't "glue together" elements of N_A . Let $f(a_A) = a_B$ and $f(b_A) = b_B$ and $a_A \neq b_A$, let's show that $a_B \neq b_B$. Let's assume the contrary: $a_B = b_B$, it is equivalent to $f(a_A) = f(b_A)$. As $a_A \neq b_A$, then without loss of generality $a_A < b_A$. According to the **main theorem**, the set N_A can be written as:

$N_A \equiv \{1_A, n(1_A), n(n(1_A)), n(n(n(1_A))), n(n(n(n(1_A)))) \dots\}$ and a_A must be on the left of b_A in this "row" (if a_A is on the right of b_A , then $b_A < a_A$, which contradicts to $a_A < b_A$), then $N_A \equiv \{1_A, n(1_A), n(n(1_A)), n(n(n(1_A))), a_A \dots b_A \dots\}$, then $b_A = n(n(\dots n(a_A)))$, then $f(b_A) = f(n(n(\dots n(a_A))))$. From the definition of f it's easy to see that it has the next property: $f(n(a_A)) = n(f(a_A))$ for any $a_A \in N_A$, then $f(n(n(\dots n(a_A)))) = n(f(n(\dots n(a_A)))) = n(n(f(\dots n(a_A)))) = n(n(\dots n(f(a_A))))$, then $f(b_A) = n(n(\dots n(f(a_A))))$, then $f(b_A) > f(a_A)$. It contradicts to the assumption $f(a_A) = f(b_A)$, then $f(a_A) \neq f(b_A)$.

From the **[Step1]+[Step2]+[Step3]** follows that $f : N_A \rightarrow N_B$ is one-to-one mapping.

[Step4] Let's show that N_A is isomorphic to N_B , i.e., $a_A < b_A$ (in N_A) $\Rightarrow f(a_A) < f(b_A)$ (in N_B) [V]. The proof of [V] is done in the **[Step3]**.

Comment. It's very easy to show that from [V] immediately follows the converse one:

$f(a_A) < f(b_A)$ (in N_B) $\Rightarrow a_A < b_A$ (in N_A). Let's fix any $f(a_A) < f(b_A)$. As $a_A, b_A \in N_A$, then exactly one of the next cases is true: $a_A = b_A$, or $a_A > b_A$, or $a_A < b_A$. If $a_A > b_A$, then (acc. to [V]) there must be $f(a_A) > f(b_A)$, which is not true. If $a_A = b_A$, then there must be $f(a_A) = f(b_A)$, which is not true. Then the only possible variant is $a_A < b_A$. And similarly for any other ordered sets.

Multiplication

Def. Multiplication " \cdot " of natural numbers is the binary operation $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ such that:

[A] $a \cdot 1 = a \quad \forall a \in \mathbb{N}$, **[B]** $a \cdot n(b) = a \cdot b + a \quad \forall a, b \in \mathbb{N}$.

Note: **[B]** can be rewritten as $a \cdot (b + 1) = a \cdot b + a \quad \forall a, b \in \mathbb{N}$.

Let's show that this definition is correct, i.e., there exist the unique operation with these properties.

Existence. Let's take 1 and define the multiplication " \bullet^1 " on the set of pairs $\{(1, b) \mid b \in \mathbb{N}\}$,

where 1 is fixed and b is an arbitrary natural number, so $1 \bullet^1 b \equiv /by\ def / \equiv b$.

We need to check that " \bullet^1 " is a multiplication in the case $a \equiv 1$. So $1 \bullet^1 1 = 1$ (property **[A]**) and

$1 \bullet^1 n(b) = n(b) = b + 1 = 1 \bullet^1 b + 1$ (property **[B]**).

Let M is the set of all natural numbers a , for every of which there exist it's own multiplication

" \bullet^a ", which is defined on the set of all pairs $\{(a, b) \mid b \in \mathbb{N}\}$ and satisfies to **[A]** and **[B]**.

We will show that $M = \mathbb{N}$. **[A]** $1 \in M$ (as were shown above) **[B]** If some $a \in M$, then it has it's own

multiplication " \bullet^a ", which is defined on the set of all pairs $\{(a, b) \mid b \in \mathbb{N}\}$ such that **[A]** and **[B]**.

Let's take the next element $n(a)$ and define for it it's own multiplication " $\bullet^{n(a)}$ " on the set

$\{(n(a), b) \mid b \in \mathbb{N}\}$. We define: $n(a) \bullet^{n(a)} b \equiv /by\ def / \equiv a \bullet^a b + b$.

Then $n(a) \bullet^{n(a)} 1 = a \bullet^a 1 + 1 = a + 1 = n(a)$ (property **[A]**)

$n(a) \bullet^{n(a)} n(b) = a \bullet^a n(b) + n(b) = (a \bullet^a b + a) + n(b) = a \bullet^a b + (a + n(b)) =$

$= a \bullet^a b + n(a + b) = a \bullet^a b + n(b + a) = a \bullet^a b + (b + n(a)) = (a \bullet^a b + b) + n(a) = n(a) \bullet^{n(a)} b + n(a)$

(property **[B]**). By the **induction axiom** $M = \mathbb{N}$, so for any a there exists it's own multiplication " \bullet^a ".

Let's define the ordinary multiplication " \cdot " on every pair (a, b) .

By definition $a \cdot b \equiv /by\ def / \equiv a \bullet^a b$. Then " \cdot " satisfies to **[A]** and **[B]**. The existence is proved.

Uniqueness. Let's show that the operation " \cdot " is unique. We assume that there exist some other

binary operation $\otimes: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ with the properties **[A]** and **[B]**. We will show that

$a \cdot b = a \otimes b \quad \forall a, b \in \mathbb{N}$, then " \cdot " = " \otimes ". Let's fix an arbitrary $a \in \mathbb{N}$. And M -is the set of all b such that $a \cdot b = a \otimes b$.

[A] $1 \in M$. Really, according to **[A]**, $a \cdot 1 = a$ and $a \otimes 1 = a$, therefore $a \cdot 1 = a \otimes 1$.

[B] If some $b \in M$, then $a \cdot b = a \otimes b$. Let's consider

$a \cdot n(b) = a \cdot b + b = //\ as \ a \cdot b = a \otimes b // = a \otimes b + b = a \otimes n(b)$, therefore $n(b) \in M$.

By the induction axiom $M = \mathbb{N}$ and therefore $a \cdot b = a \otimes b$ for any $b \in \mathbb{N}$, where a is an arbitrary fixed number, then $a \cdot b = a \otimes b$ for any $a, b \in \mathbb{N}$.

Before we prove the basic properties of multiplication we need an auxiliary lemma.

Lemma6. Right distributivity $(a+b) \cdot c = a \cdot c + b \cdot c$. Let's fix arbitrary numbers $a, b \in \mathbb{N}$.

And M is the set of all c , for which the formula $(a+b) \cdot c = a \cdot c + b \cdot c$ is true.

[A] obviously $1 \in M$ [B] If some $c \in M$, then $(a+b) \cdot c = a \cdot c + b \cdot c$.

Let's consider $(a+b) \cdot n(c) = // \text{property [B]} // =$

$= (a+b) \cdot c + (a+b) = (a \cdot c + b \cdot c) + (a+b) = (a \cdot c + a) + (b \cdot c + b) = // \text{property [B]} // =$

$= a \cdot n(c) + b \cdot n(c)$, then $n(c) \in M$, so $M = \mathbb{N}$. As a, b are arbitrary fixed natural numbers, then the right distributivity is true for any $a, b, c \in \mathbb{N}$.

Commutativity. $a \cdot b = b \cdot a$ for any $a, b \in \mathbb{N}$.

Step one. Commutativity for one. Let $b \equiv 1$. Let's show that $a \cdot 1 = 1 \cdot a$ for any $a \in \mathbb{N}$. Let M is the set of all numbers a , for which $a \cdot 1 = 1 \cdot a$. [A] $1 \in M$, because $1 \cdot 1 = 1 \cdot 1 = 1$ (property [A]),

[B] If some $a \in M$, then $a \cdot 1 = 1 \cdot a$. Let's consider

$1 \cdot n(a) = 1 \cdot a + 1 = a \cdot 1 + 1 = / \text{right distributivity} / = (a+1) \cdot 1 = n(a) \cdot 1$, therefore $n(a) \in M$.

So $M = \mathbb{N}$. And we are going to the step two.

Step Two. General commutativity. Let's fix an arbitrary $a \in \mathbb{N}$. Let M is the set of all b , for which $a \cdot b = b \cdot a$. [A] $1 \in M$ (step one), [B] If $b \in M$, then $a \cdot b = b \cdot a$. Let's consider

$a \cdot n(b) = a \cdot b + a = b \cdot a + a = / \text{right distributivity} / = (b+1) \cdot a = n(b) \cdot a$ then $n(b) \in M$.

Then $M = \mathbb{N}$. And everything is proved.

Consequences.

[A] General distributivity: $(a+b) \cdot c = c \cdot (a+b) = a \cdot c + b \cdot c = c \cdot a + c \cdot b$

(follows from [commutativity](#) and [lemma6](#)).

[B] Distributive law for subtraction: $(a-b) \cdot c = c \cdot (a-b) = a \cdot c - b \cdot c = c \cdot a - c \cdot b$ for any $a, b, c \in \mathbb{N}$ where $a > b$.

Proof. Let $a-b = \Delta$, by the definition of subtraction it means that $a = b + \Delta$, then [a]

$(a-b) \cdot c = \Delta \cdot c$ and [b] $a \cdot c - b \cdot c = (b + \Delta) \cdot c - b \cdot c = (b \cdot c + \Delta \cdot c) - b \cdot c = \Delta \cdot c$.

From [a] and [b] we see that $(a-b) \cdot c = a \cdot c - b \cdot c$. The rest follows from commutativity of ".".

Associativity. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any $a, b, c \in \mathbb{N}$. Let's fix arbitrary $a, b \in \mathbb{N}$. And M is the set of all c , for which $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. [A] $1 \in M$. Really, $(a \cdot b) \cdot 1 = a \cdot b = a \cdot (b \cdot 1)$, [B] If $c \in M$, then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Let's consider $(a \cdot b) \cdot n(c) = / \text{property [B]} / = (a \cdot b) \cdot c + (a \cdot b) =$

$= a \cdot (b \cdot c) + a \cdot b = // \text{left distributivity} // = a \cdot (b \cdot c + b) = // \text{left distributivity} // =$

$= a \cdot (b \cdot (c+1)) = a \cdot (b \cdot n(c))$. Then $n(c) \in M$. Then $M = \mathbb{N}$.

Exercise 1. Prove the next basic properties (If there is a difference $a - b$ or $c - d$, then $a > b$ and $c > d$) **[A]** $(a + b) \cdot (c + d) = (a \cdot c + a \cdot d) + (b \cdot c + b \cdot d)$ and $(a + b) \cdot (c - d) = (a \cdot c - a \cdot d) + (b \cdot c - b \cdot d)$ and $(a - b) \cdot (c - d) = (a \cdot c - a \cdot d) - (b \cdot c - b \cdot d)$

[B] $a \cdot c = b \cdot c \Leftrightarrow a = b$ and $a \cdot c > b \cdot c \Leftrightarrow a > b$
 $a + c = b + c \Leftrightarrow a = b$ and $a + c > b + c \Leftrightarrow a > b$.

[C] $a > b, c > d \Rightarrow a \cdot c > b \cdot d, a + c > b + d$.

Let's show for example that $(a + b) \cdot (c + d) = (a \cdot c + a \cdot d) + (b \cdot c + b \cdot d)$. Let's take the expression $(a + b) \cdot (c + d)$. We can consider $(a + b)$ as a sum of two numbers and $(c + d)$ as a separate number. Then $(a + b) \cdot (c + d) = a \cdot (c + d) + b \cdot (c + d) = (a \cdot c + a \cdot d) + (b \cdot c + b \cdot d)$.

Let's show $(a - b) \cdot (c - d) = (a \cdot c - a \cdot d) - (b \cdot c - b \cdot d)$. Let $a - b = \Delta$ and $c - d = \delta$, then $a = b + \Delta$ and $c = d + \delta$. So the left part equals $(a - b) \cdot (c - d) = \Delta \cdot \delta$.

The right part is

$$(a \cdot c - a \cdot d) - (b \cdot c - b \cdot d) = [a \cdot (c - d)] - [b \cdot (c - d)] = [a \cdot \delta] - [b \cdot \delta] = [(b + \Delta) \cdot \delta] - [b \cdot \delta] = [(b + \Delta) - b] \cdot \delta = \Delta \cdot \delta.$$

Then the left and right sides are equal.

Let's show the last one: $a > b, c > d \Rightarrow a = b + \Delta, c = d + \delta$.

Then $a \cdot c = (b + \Delta) \cdot (d + \delta) = (b \cdot d + b \cdot \delta) + (\Delta \cdot d + \Delta \cdot \delta) = b \cdot d + (b \cdot \delta + (\Delta \cdot d + \Delta \cdot \delta)) > b \cdot d$.

The part $a \cdot c > b \cdot d$ is proved. Let's show now that $a + c > b + d$.

So $a + c = (b + \Delta) + (d + \delta) = (b + d) + (\Delta + \delta) > (b + d)$.

Archimedes axiom. For any pair of natural numbers $a, b \in \mathbb{N}$ there exist $n \in \mathbb{N}$ such that $n \cdot a > b$ (this property is called an **Archimedes axiom**).

Proof. Let's fix an arbitrary pair of natural numbers a, b . Let's take $n = b + 1$, then

$$(b + 1) \cdot a = b \cdot a + a = /as a \geq 1/ \geq b \cdot 1 + 1 = b + 1 > b.$$

Notice that when we say "axiom" we usually imply some fact which must be accepted without any proofs. But for the natural numbers the Archimedes axiom is not an axiom at all, it is just one of the properties of natural numbers. So now, the "Archimedes axiom" is just a name of the certain property. Later, during the length construction, the Archimedes axiom will be the real axiom, which will be accepted without any proofs.

Division ":"

Def. Let's consider the set H of all pairs (a, b) , where a can be represented as $a = k \cdot b$ for some natural number k . Division ":" is the mapping $H \rightarrow \mathbb{N}$ that for every pair $(a, b) \in H$ compares the natural number k such that $a = k \cdot b$, for every such pair, k is called a quotient of numbers a, b , and we write $k \equiv a/b \equiv \frac{a}{b}$.

The given definition is correct: if $k = a/b$ then there is no other number $\Delta \neq k$ such that $\Delta = a/b$. Really, let there exist some other Δ . Without loss of generality $\Delta > k$. As $\Delta = a/b \Rightarrow a = \Delta \cdot b$, as $k = a/b \Rightarrow a = k \cdot b$, then $\Delta \cdot b = k \cdot b$, but $\Delta > k$, then there must be $\Delta \cdot b > k \cdot b$, we have a contradiction. So $\Delta = k$.

Exercise2. Prove next simple properties: If there is a/b or c/d , then $a = k \cdot b$ (for some $k \in \mathbb{N}$) and $c = \Delta \cdot d$ (for some $\Delta \in \mathbb{N}$). If there is $\frac{a}{b} / \frac{c}{d}$, then $\frac{a}{b} = m \cdot \frac{c}{d}$ (for some $m \in \mathbb{N}$).

$$[A] \frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d} \quad \text{and} \quad \frac{a}{b} - \frac{c}{d} = \frac{a \cdot d - b \cdot c}{b \cdot d}, \quad [B] \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d} \quad \text{and} \quad \frac{a}{b} / \frac{c}{d} = \frac{a \cdot d}{b \cdot c},$$

Exercise3.

$$[A] \frac{a}{b} = \frac{c}{d} \Leftrightarrow a \cdot d = b \cdot c, \quad [B] a > b \Leftrightarrow \frac{a}{c} > \frac{b}{c} \quad \text{and} \quad a > b \Leftrightarrow \frac{c}{a} < \frac{c}{b}, \quad [C] a \geq \frac{a}{b} \text{ for any } b \in \mathbb{N},$$

$$\text{if } b \neq e, \text{ then } a > \frac{a}{b}.$$

Advanced part.

Notice that there exist different sets of natural numbers (it's enough to change the designation of any symbol in \mathbb{N} , in order to turn it into a new set. For example, we can change the designation $1 \rightarrow \Delta$ and do not change any other numbers, then we will have the new set of natural numbers, where the symbol Δ is an element "one". Addition and multiplication of natural numbers are always binary operations which are defined on a concrete set of natural numbers.

Let N_A is a set of natural numbers, we can write $N_A \equiv (N_A, +, \cdot)$, implying that we consider the set N_A together with the addition and multiplication which are defined on it.

And similarly, $N_B \equiv (N_B, \oplus, \bullet)$. Notice that we use different symbols to define operations on N_A and N_B . Of course, the addition $+$ on N_A has the same properties as the addition \oplus on N_B , but $+$ and \oplus are different operations, because they are defined on different sets.

The same is true for multiplications \cdot, \bullet .

Advanced Theorem3. For any sets $(N_A, +, \cdot)$ and (N_B, \oplus, \bullet) of natural numbers there exist the **unique** isomorphism $f : N_A \rightarrow N_B$ (where f is an isomorphism of ordered sets).

Moreover, f has the next properties: **[T]**

$$a_A + b_A = c_A \text{ (in } N_A) \Rightarrow f(a_A) \oplus f(b_A) = f(c_A) \text{ (in } N_B) \text{ and}$$

$$a_A \cdot b_A = d_A \text{ (in } N_A) \Rightarrow f(a_A) \bullet f(b_A) = f(d_A) \text{ (in } N_B).$$

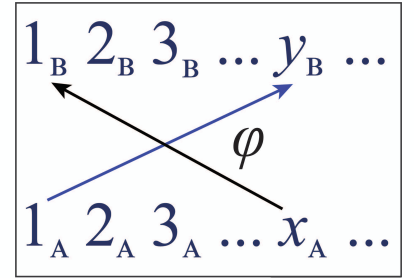
Proof. The existence of f and even the explicit definition of f are provided in the **theorem3**.

Let's assume that there exist some other isomorphism $\varphi : N_A \rightarrow N_B$ (where φ is also an isomorphism of ordered sets, so **there must be:** **[A]** φ is one-to-one and

[B] $a < b \text{ (in } N_A) \Leftrightarrow f(a) < f(b) \text{ (in } N_B)$). Let's show that $f(a) = \varphi(a) \forall a \in N_A$, then $f \equiv \varphi$ and f is unique.

The main auxiliary lemma. φ has exactly the same properties as f : it transfers one into one $\varphi(1_A) = 1_B$ and **if** $\varphi(a_A) = a_B$, **then** $\varphi(n(a_A)) = n(a_B)$.

Proof. Let's show that $\varphi(1_A) = 1_B$. We consider $\varphi(1_A)$, let $\varphi(1_A) \neq 1_B$, then $\varphi(1_A) = y_B$, where y_B is some element of N_B . We know that φ is one-to-one, so the element $1_B \in N_B$ must have some preimage $x_A \in N_A$: $\varphi(x_A) \equiv 1_B$. Then we have two equalities: $\varphi(1_A) = y_B$ and $\varphi(x_A) \equiv 1_B$ **[pict8]**. The one 1_A is the least number in N_A , then $1_A < x_A$. Then $\varphi(1_A) < \varphi(x_A)$ (look now at our equalities), then $y_B < 1_B$ and we have a contradiction. Then $\varphi(1_A) = 1_B$.



pict.8

Let's show that the condition “**if** $\varphi(a_A) = a_B$, **then** $\varphi(n(a_A)) = n(a_B)$ ” **[V]** is true for any $a_A \in N_A$

Let M_A is the set of all a_A , for which **[V]** is true.

[A] $1_A \in M$. We have $\varphi(1_A) = 1_B$, let's show that $\varphi(2_A) = 2_B$. We will show that $\varphi(2_A)$ can be equal only to 2_B . Really, $1_A < 2_A \Rightarrow \varphi(1_A) < \varphi(2_A) \Leftrightarrow 1_B < \varphi(2_A)$. **If** the value $\varphi(2_A) = 2_B$, then

[A] is proved. Let's assume that $\varphi(2_A) = y_B > 2_B$, then, anyway there

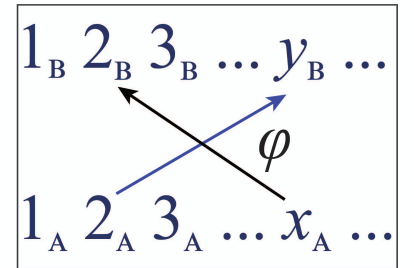
must be some element $x_A \in N_A$ such that $\varphi(x_A) = 2_B$ and

$x_A \neq 1_A, x_A \neq 2_A \Rightarrow x_A > 2_A$. Then we have: $\varphi(2_A) = y_B \parallel y_B > 2_B$ and

$\varphi(x_A) = 2_B \parallel x_A > 2_A$ **[pict9]**, here we have a contradiction, really

$x_A > 2_A$, then there must be $\varphi(x_A) > \varphi(2_A) \Leftrightarrow 2_B > y_B$, but $y_B > 2_B$.

So $\varphi(2_A)$ can be equal only to 2_B , and **[A]** is proved.



pict.9

[B] If $a_A \in M_A$, it means that we have $\varphi(a_A) = a_B$ and $\varphi(n(a_A)) = n(a_B)$. We need to show that the similar condition is true for $n(a_A)$. We already have $\varphi(n(a_A)) = n(a_B)$, then we **need to show** that $\varphi(n[n(a_A)]) = n[n(a_B)]$. It's not difficult to do, by using an auxiliary picture (like pictures 8,9). Perform it as a simple exercise. After it's done, by the induction axiom, [V] is proved.

Let's prove now the **auxiliary lemma**. Let M_A is the set of all natural numbers a_A , for which $f(a_A) = \varphi(a_A)$.

[A] $1_A \in M$. Because $\varphi(1_A) = 1_B$ and $f(1_A) = 1_B$. [B] If $a_A \in M_A$ then $f(a_A) = \varphi(a_A)$.

We want to show that $f(n(a_A)) = \varphi(n(a_A))$. From the basic properties of these isomorphisms we have $f(n(a_A)) = n(f(a_A))$ and $\varphi(n(a_A)) = n(\varphi(a_A))$. As the elements $f(a_A)$ and $\varphi(a_A)$ are equal, then the elements $n(f(a_A))$ and $n(\varphi(a_A))$ are also equal, therefore $f(n(a_A)) = \varphi(n(a_A))$. And $n(a_A) \in M_A$. So $M_A = N_A$ and $f \equiv \varphi$ on N_A .

Let's prove the properties [T]. These properties are obviously equivalent to

[T_p]: $f(a_A + b_A) = f(a_A) \oplus f(b_A)$ and $f(a_A \cdot b_A) = f(a_A) \bullet f(b_A)$ for any $a_A, b_A \in N_A$.

Let's prove **the first one**. We fix an arbitrary $a_A \in N_A$. Let M_A is the set of all numbers b_A , for which $f(a_A + b_A) = f(a_A) \oplus f(b_A)$.

[A] $1_A \in M_A$. Really $f(a_A + 1_A) = f(n(a_A)) = n(f(a_A)) = f(a_A) \oplus 1_B = f(a_A) \oplus f(1_A)$, so $1_A \in M$.

[B] If $b_A \in M$, then $f(a_A + b_A) = f(a_A) \oplus f(b_A)$. Let's consider $f(a_A + n(b_A)) = f(n(a_A + b_A)) = n(f(a_A + b_A)) = n(f(a_A) \oplus f(b_A)) = f(a_A) \oplus n(f(b_A)) = f(a_A) \oplus f(n(b_A))$ (we used the basic properties of the addition $+$ on N_A and \oplus on N_B), so $n(b_A) \in M_A$, then $M_A = N_A$ and the property $f(a_A + b_A) = f(a_A) \oplus f(b_A)$ is proved.

Let's prove **the second one**: $f(a_A \cdot b_A) = f(a_A) \bullet f(b_A)$. We fix again an arbitrary $a_A \in N_A$ and M_A is the set of all numbers b_A , for which $f(a_A \cdot b_A) = f(a_A) \bullet f(b_A)$.

[A] $1_A \in M$. Really $f(a_A \cdot 1_A) = f(a_A) = f(a_A) \bullet 1_B = f(a_A) \bullet f(1_A)$.


[B] If $b_A \in M$, then $f(a_A \cdot b_A) = f(a_A) \bullet f(b_A)$. Let's consider

$f(a_A \cdot n(b_A)) = f(a_A \cdot b_A + a_A) = f(a_A \cdot b_A) \oplus f(a_A) = f(a_A) \bullet f(b_A) \oplus f(a_A) = // \text{distributivity} // = f(a_A) \bullet (f(b_A) \oplus 1_B) = f(a_A) \bullet (f(b_A) \oplus f(1_A)) = f(a_A) \bullet f(b_A + 1_A) = f(a_A) \bullet f(n(b_A))$,

then $n(b_A) \in M_A$ and $M_A = N_A$. Everything is proved.



2



*Groups, rings,
fields*

Multiplicative groups

Def. G is a set with a binary operation $\cdot: G \times G \rightarrow G$ “multiplication”.

And **[A]** Multiplication is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any $a, b, c \in G$.

[B] There exist the element “one” e such that $a \cdot e = e \cdot a$ for any $a \in G$.

[C] For any element $a \in G$ there exist the inverse element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.
Then G is called a multiplicative group, or just a group.

As \cdot is associative (**The main theorem2**, page 23), then in any expression with any arrangement of brackets we can rearrange brackets in any way we want, it will not change an expression.

For example: $(a \cdot c) \cdot (d \cdot (v \cdot m)) = (a \cdot c \cdot d) \cdot v \cdot m$.

Property. For any element $a \in G$, an inverse element $a^{-1} \in G$ is always unique.

Let's fix any $a \in G$. According to **[C]**, there exist at least one inverse element a^{-1} . If there is some other inverse element $b \in G$, then $a \cdot a^{-1} = e$ and $a \cdot b = e$, then $a \cdot a^{-1} = a \cdot b$. Let's multiply both sides by a^{-1} from the left side, then $a^{-1} \cdot (a \cdot a^{-1}) = a^{-1} \cdot (a \cdot b) \Leftrightarrow [\text{associativity}] \Leftrightarrow (a^{-1} \cdot a) \cdot a^{-1} = (a^{-1} \cdot a) \cdot b \Leftrightarrow e \cdot a^{-1} = e \cdot b \Leftrightarrow a^{-1} = b$, it proves the uniqueness.

Def: a subset $H \subset G$ is called a subgroup of G if H is closed under multiplication and H is a group. When we say “ H is closed under multiplication”, we mean that for any $a, b \in H$ there must be $a \cdot b \in H$. And when we say “ H is a group”, we mean that the properties **[A]**, **[B]**, **[C]** are true for any elements of H .

Subgroup criterion. $H \subset G$ is a subgroup \Leftrightarrow for any $a, b \in H$ there is $a \cdot b \in H$ and $a^{-1} \in H$.

Proof. \Rightarrow if H is a subgroup of G , then obviously $a \cdot b \in H$ and $a^{-1} \in H$.

\Leftarrow From $a \cdot b \in H$ follows that H is closed under multiplication. Let's take any $a \in H$, then $a^{-1} \in H$, then **[C]** is true for H . And $a \cdot a^{-1} = e \in H$, so **[B]** is true for H .

Then H is a subgroup of G . (The property **[A]** is always true for any elements of G , so there is nothing to check).

From this criterion immediately follows that any subgroup $H \subset G$ must contain an element one “ e ”, moreover, the subgroup which consists of only one element $\{e\}$ is a minimal subgroup of G , and the subgroup $H = G$ is a maximal subgroup of G .

A group G is called commutative if the operation $\cdot: G \times G \rightarrow G$ is commutative: $a \cdot b = b \cdot a$ for any $a, b \in G$. In any commutative group we can speak about division “/”.

Def. G is a commutative multiplicative group.

Division “/” is the binary operation $/: G \times G \rightarrow G$ that for any pair $a, b \in G$ compares the element $x \equiv (a/b) \equiv \frac{a}{b}$ such that $a = x \cdot b = b \cdot x$.

The given definition is correct. For any $a, b \in G$ there exist the unique element x such that $a = x \cdot b = b \cdot x$.

Let's consider $a = x \cdot b$ as an equation, we multiply both sides by b^{-1} from the right side:

$a \cdot b^{-1} = (x \cdot b) \cdot b^{-1} \Rightarrow / \text{associativity} / \Rightarrow a \cdot b^{-1} = x \cdot (b \cdot b^{-1}) \Rightarrow x = a \cdot b^{-1}$, and it's easy to check that x really satisfies to $a = x \cdot b = b \cdot x$. The existence is proved, the uniqueness is obvious.

Exercise1. G is an multiplicative commutative group, then the next properties are true for any elements of G **[A]** $\frac{a}{a} = e$ and $a \cdot \frac{e}{a} = e$ and $a \cdot \frac{e}{b} = \frac{a}{b}$ and $\frac{a}{b} \cdot \frac{b}{a} = e$ and $a \cdot b = c \cdot b \Leftrightarrow a = c$.

[B] $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$ and $\frac{a}{b} \bigg/ \frac{c}{d} = \frac{a \cdot d}{b \cdot c}$.

Additive groups (everything is very similar here).

Def. G is a set with a binary operation "+": $G \times G \rightarrow G$ "addition".

And **[A]** Addition is associative: $(a + b) + c = a + (b + c)$ for any $a, b, c \in G$.

[B] There exist the element "zero" 0 such that $a + 0 = 0 + a$ for any $a \in G$.

[C] For any element $a \in G$ there exist the inverse element $-a \in G$ such that $a + (-a) = (-a) + a = 0$.

Then G is called an additive group, or just a group.

Def: a subset $H \subset G$ is called a subgroup of G if H is closed under addition and H is a group. I.e.: for any $a, b \in H$ there must be $(a + b) \in H$. And the properties **[A]**, **[B]**, **[C]** are true for any elements of H .

Subgroup criterion. $H \subset G$ is a subgroup \Leftrightarrow for any $a, b \in H$ there is $a + b \in H$ and $-a \in H$.

In any commutative additive group G we can speak about subtraction "-": $G \times G \rightarrow G$.

For any $a, b \in G$, the element $x \equiv (a - b)$ is such element that $a = (a - b) + b = b + (a - b)$.

Exercise2: G is an additive commutative group, then the next properties are true for any elements of G (compare with the **exercise1**):

[A] $a - a = 0$ and $a + (-a) = 0$ and $a + (-b) = a - b$ and $(a - b) + (b - a) = 0$

and $a + b = c + b \Leftrightarrow a = c$,

[B] $(a - b) + (c - d) = (a + c) - (b + d)$ and $(a - b) - (c - d) = (a + d) - (b + c)$.

It's easy to notice that there is no essential difference between additive and multiplicative groups.

In general, a group G with a binary operation \circ is denoted like (G, \circ)

Def. We say that (G, \circ) is isomorphic to (D, \bullet) if there exist some one-to-one mapping $f : G \rightarrow D$ such that: if $a \circ b = c$ (in G), then $f(a) \bullet f(b) = f(c)$ (in D).

Property. If (G, \circ) is isomorphic to (D, \bullet) , then (D, \bullet) is isomorphic to (G, \circ) .

Proof. Let there exist one-to-one $f : G \rightarrow D$ with such property. Let's consider the inverse mapping $f^{-1} : D \rightarrow G$. We need to show that if $\omega \bullet \eta = \mu$ (in D), then $f^{-1}(\omega) \circ f^{-1}(\eta) = f^{-1}(\mu)$ (in G).

Every element $\omega \in D$ can be uniquely represented as $\omega = f(a)$ for some $a \in G$, then the equality $\omega \bullet \eta = \mu$ is equivalent to $f(a) \bullet f(b) = f(c)$, where a, b, c are some elements of G .

We want to show that $f^{-1}(\omega) \circ f^{-1}(\eta) = f^{-1}(\mu)$ and it is equivalent to $f^{-1}(f(a)) \circ f^{-1}(f(b)) = f^{-1}(f(c)) \Leftrightarrow a \circ b = c$.

Let's sum up: we need to show that from $f(a) \bullet f(b) = f(c)$ follows that $a \circ b = c$.

Let's assume the contrary $a \circ b \neq c$, then $a \circ b = d$ (where $d \neq c$). According to the main property of f : if $a \circ b = d$, then $f(a) \bullet f(b) = f(d)$, therefore $f(c) = f(d)$. As f is one-to-one, then $c = d$, and we have a contradiction. Therefore, if $f(a) \bullet f(b) = f(c)$, then $a \circ b = c$ which is equivalent to: if $\omega \bullet \eta = \mu$ (in D), then $f^{-1}(\omega) \circ f^{-1}(\eta) = f^{-1}(\mu)$ (in D). And f^{-1} is an isomorphism.

From this property follows that if one group is isomorphic to the other, then we can just say "groups are isomorphic". Any two isomorphic groups are almost identical, there is one-to-one correspondence between their elements, and if elements of one group are connected by some relation (like one element is a product of others), then their images/preimages in the other group are connected by exactly the same relation.

For practical purposes (when we want to show that two groups are isomorphic) it's easier to use the other, equivalent definition.

Def. (G, \circ) is isomorphic to (D, \bullet) if there exist one-to-one mapping $f : G \rightarrow D$ such that $f(a \circ b) = f(a) \bullet f(b)$ for any $a, b \in G$.

Show that this definition is equivalent to the initial one. From here follows (understand why) that this definition is also symmetric: if (G, \circ) is isomorphic to (D, \bullet) (according to this definition), then (D, \bullet) is isomorphic to (G, \circ) .

When groups are isomorphic we write $(G, \circ) \cong (D, \bullet)$, or just $G \cong D$.

Exercise3. f is an isomorphism of groups (G, \circ) and (D, \bullet) . Then "one always goes to one" $f(e_G) = e_D$. And for any $a \in G$ we have $f(a^{-1}) = f(a)^{-1}$.

Solution. Any element $d \in D$ has the unique representation as $d = f(a) \parallel a \in G$, then for any $d \in D$ we have $d \bullet f(e_G) = f(a) \bullet f(e_G) = f(a \circ e_G) = f(a) = d$, so $d \bullet f(e_G) = d$ for any $d \in D$ and similarly $f(e_G) \bullet d = d$, then $f(e_G)$ is a one of the group D , so $f(e_G) = e_D$.

Let's fix now an arbitrary $a \in G$. Let's take $f(a^{-1})$ and consider the product:

$f(a^{-1}) \bullet f(a) = f(a^{-1} \circ a) = f(e_G) = e_D$. By definition, $f(a)^{-1}$ is such element that

$f(a^{-1}) \bullet f(a) = e_D$, then $f(a^{-1}) \bullet f(a) = f(a)^{-1} \bullet f(a)$. Let's multiply both sides of the last equality by $f(a)^{-1}$ from the right side, then $f(a^{-1}) = f(a)^{-1}$.

Def. G is a group. For any $a \in G$ and for any natural number $n \in \mathbb{N}$ let's define the element: $na \equiv a + a + \dots + a$ (there are exactly n summands on the right side). If G is a multiplicative group, then for any $a \in G$ and for any natural number $n \in \mathbb{N}$ we define $a^n \equiv a \cdot a \cdot \dots \cdot a$ (there are exactly n factors on the right side).

Then in any **commutative** additive group, for any elements a, b and any natural numbers m, n :

[A] $ma + na = (m + n)a$ **[B]** $m(a + b) = ma + mb$ **[C]** $mna = n(ma) = m(na)$ **[D]** $-(ma) = m(-a)$

In any **commutative** multiplicative group, for any elements a, b and any natural numbers m, n :

[A] $a^m \cdot a^n = a^{m+n}$ **[B]** $(a \cdot b)^m = a^m \cdot b^m$ **[C]** $a^{mn} = (a^m)^n = (a^n)^m$ **[D]** $(a^m)^{-1} = (a^{-1})^m$.

Def. R is a set with two binary operations on it: addition "+" and multiplication ".".

[A] R is a commutative group with respect to addition "+",

[B] Multiplication "." is associative. And there is a distributive law: $(a + b) \cdot c = a \cdot c + b \cdot c$ and $c \cdot (a + b) = c \cdot a + c \cdot b$ for any $a, b, c \in R$

Then R is called a ring.

Notice that multiplication mustn't be commutative, there may no be the element "one" $e \in R$ such that $a \cdot e = e \cdot a = a$ (for any $a \in R$). If multiplication is commutative, we say " R is a commutative ring". If there exist an element "one" $e \in R$, then we say " R is a ring with one".

And we can say for example: " R is a commutative ring with one". Any ring R is a commutative group with respect to addition and therefore, subtraction is defined on R .

Property1. In any ring R the distributive law for subtraction is true:

$a \cdot (b - c) = a \cdot b - a \cdot c$ and $(a - b) \cdot c = a \cdot c - b \cdot c$ for any $a, b, c \in R$.

Proof. Let's show that $a \cdot (b - c) = a \cdot b - a \cdot c$ **[a]**. This equality is equivalent to

$a \cdot (b - c) + a \cdot c = a \cdot b$, let's simplify the left part:

$a \cdot (b - c) + a \cdot c = / \text{ordinary distributivity} / = a \cdot ((b - c) + c) = a \cdot b$ and **[a]** is true.

The proof of the other formula is similar.

Consequence. In any ring R , for any element $a \in R$ we have $a \cdot 0 = 0 \cdot a = 0$.

Proof. Let's fix an arbitrary $a \in R$, then $a \cdot 0 = a \cdot (a - a) = / \text{property 1} / = a \cdot a - a \cdot a = 0$

Exercise4. R is a ring. Then for any $a, b, c, d \in R$:

[A] $a \cdot (-b) = -a \cdot b$ and $(-a) \cdot b = -a \cdot b$ and $(-a) \cdot (-b) = a \cdot b$,

[B] $(a + b) \cdot (c + d) = (a \cdot c + a \cdot d) + (b \cdot c + b \cdot d)$ and $(a - b) \cdot (c + d) = (a \cdot c + a \cdot d) - (b \cdot c + b \cdot d)$ and $(a + b) \cdot (c - d) = (a \cdot c + b \cdot c) - (a \cdot d + b \cdot d)$ and $(a - b) \cdot (c - d) = (a \cdot c + b \cdot d) - (a \cdot d + b \cdot c)$,

[C] If R is a commutative ring, then the next well known formulas are true:

$$a^2 - b^2 = (a - b) \cdot (a + b) \quad \text{and} \quad (a + b)^2 = a^2 + 2 \cdot a \cdot b + b^2 \quad \text{and}$$

$$(a + b)^3 = a^3 + 3 \cdot a \cdot b^2 + 3 \cdot b^2 \cdot a + b^3.$$

Def: a set $H \subset R$ is called a subring of R if H is closed with respect to addition "+" and multiplication "." and H is a ring.

When we say that H is closed with respect to "+" and "." we mean that
 $\forall a, b \in H \Rightarrow a + b \in H, \quad a \cdot b \in H.$

When we say that H is a ring, we mean that H satisfies to the ring-definition.

Subring criterion. R is a ring.

$$H \subset R \text{ is a subring of } R \Leftrightarrow \forall a, b \in H: a + b \in H, \quad a - b \in H, \quad a \cdot b \in H.$$

Def: a ring F is called a field if all nonzero elements of F form a commutative group with respect to multiplication ".".

Notice that any field is also a ring (by **definition**), but it is such ring, where all nonzero elements form a commutative group with respect to multiplication.

Even if F is a commutative ring with one, we can't assert that F is a field. There is no guarantee that for any nonzero element $a \in F$ there exist an inverse element $a^{-1} \in F: a \cdot a^{-1} = a^{-1} \cdot a = e$. The ring of integer numbers \mathbb{Z} (that we will build very soon) will be an exactly such type of ring: a commutative ring with one. But \mathbb{Z} is not a field.

Def. F is a field. All elements of F form a commutative group with respect to addition "+", which is called an additive group of F . All **non-zero** elements of F form a commutative group with respect to multiplication ".", which is called a multiplicative group of F .

From this definition we see that multiplication is commutative on $F \setminus \{0\}$. But it's very easy to understand that multiplication is commutative on all F . Really, let's consider the equality $a \cdot b = b \cdot a$, if one of the elements a or b is zero, then both sides of the equality are zeroes and therefore the equality is true for any $a, b \in F$.

Def. Elements a, b of a ring/field are called zero divisors if $a \cdot b = 0$, where $a \neq 0$ and $b \neq 0$, or if $b \cdot a = 0$, where $b \neq 0$ and $a \neq 0$.

There is a very important fundamental difference between rings and fields. In general, there can be some zero divisors in a ring, but there are no divisors in any field.

Let $a \cdot b = 0$ in some field F , where $a \neq 0$ and $b \neq 0$. Let's multiply both sides by a^{-1} from the left side, so $(a \cdot b) = 0 \Rightarrow a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \Rightarrow (a^{-1} \cdot a) \cdot b = 0 \Rightarrow b = 0$ - it contradicts to $b \neq 0$.

So, there are no divisors of zero in any field F .

Before we start working with fields we have to make one **very important restriction**.

As non-zero elements of F form a commutative group with respect to multiplication, division ":"

is defined on $F \setminus \{0\}$. Let's "extend" this operation to F . For any $a \neq 0$ we define $\frac{0}{a} \equiv 0$, it is reasonable, because $0 = a \cdot 0 = a \cdot 0$.

And our restriction is: for any $a \in F$, the element $\frac{a}{0}$ is **not defined**. In other words:

It is forbidden to divide by zero. Really, let $a \neq 0$ if we define $\frac{a}{0} \equiv b$, then it's reasonable to require: $a = b \cdot 0 = 0 \cdot b = 0$, then $a = 0$, but $a \neq 0$, and we have the contradiction. Therefore, we make an agreement that $\frac{a}{0}$ is **not defined** for any $a \in F$ (even for $a = 0$, the element $\frac{0}{0}$ is not defined).

Exercise 5. R is a field. Then for any $a, b, c, d \in R$ (if there is $\frac{a}{b}$ or $\frac{c}{d}$, then $b \neq 0$ and $d \neq 0$).

$$[A] \quad \frac{-a}{b} = -\frac{a}{b} \quad \text{and} \quad \frac{a}{-b} = -\frac{a}{b} \quad \text{and} \quad \frac{-a}{-b} = \frac{a}{b} \quad [B] \quad \frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d} \quad \text{and} \quad \frac{a}{b} - \frac{c}{d} = \frac{a \cdot d - b \cdot c}{b \cdot d}.$$

This theory will give us a great advantage in the future. Suppose that we deduced that some structure (some set with "+" ".") is a ring, then all the properties from the **exercises 2,4** are true for the elements of that set. Similarly, if we deduced that some structure is a field, then all the properties from the **exercises 1,2,4,5** are true for the elements of that set.

Def: a set $H \subset F$ is called a subfield of F if H is closed with respect to addition "+" and multiplication "." and H is a field.

Subfield criterion. F is a field. $H \subset F$ is a subfield of $F \Leftrightarrow$

$$\forall a, b \in H: a + b \in H, a - b \in H, a \cdot b \in H, \frac{a}{b} \in H.$$

Notice that "addition" and "multiplication" are just conditional names of some binary operations $R \times R \rightarrow R$. A ring/field R with two binary operations on it can be denoted as $(R, +, \cdot)$.

For different rings/fields these operations may have absolutely different meaning.

Def. Let $(R, +, \cdot)$ and (D, \oplus, \bullet) are two rings (fields). We say that R is isomorphic to D if there exist one-to-one mapping $f: R \rightarrow D$ such that:

[A] If $a + b = c$ (in R), then $f(a) \oplus f(b) = f(c)$ (in D).

[B] If $a \cdot b = d$ (in R), then $f(a) \bullet f(b) = f(d)$ (in D).

Property. If R is isomorphic to D , then D is isomorphic to R (the proof here is very similar to the proof that we made for groups).

And again, from this definition follows that if one ring/field is isomorphic to the other, then we can just say "these rings/fields are isomorphic".

In practice we will use the next equivalent definition.

Def. Let $(R, +, \cdot)$ and (D, \oplus, \bullet) are two rings (fields). R is isomorphic to D if there exist one-to-one mapping $f: R \rightarrow D$ such that $f(a+b) = f(a) \oplus f(b)$ and $f(a \cdot b) = f(a) \bullet f(b)$ for any $a, b \in R$.

Isomorphic rings/fields are almost identical, there is one-to-one correspondence between their elements and if some elements in one ring are connected by some relation (like one element is a sum/product of others), then their images/preimages in the other ring are connected by exactly the same relation. When rings/fields are isomorphic, we write $(R, +, \cdot) \cong (D, \oplus, \bullet)$, or just $R \cong D$. The next theorem will be repeatedly used during the construction process.

Theorem4. $(R, +, \cdot)$ is a ring/field and $[D, \oplus, \bullet]$ is some set with two (binary) operations on it: “addition” \oplus and “multiplication” \bullet (there are just some binary operations on D , we do not even need to know anything about their properties). If there exist one-to-one mapping $f: R \rightarrow D$ such that $f(a+b) = f(a) \oplus f(b)$ and $f(a \cdot b) = f(a) \bullet f(b)$ for any $a, b \in R$, **THEN** $[D, \oplus, \bullet]$ is also a ring/field.

But at first we need to prove the next auxiliary lemma.

Lemma6. (G, \cdot) is a multiplicative group and $[D, \bullet]$ is some set with a binary operation “ \bullet ”: $D \times D \rightarrow D$ on it. And there exist one-to-one mapping $f: G \rightarrow D$ such that $f(a \cdot b) = f(a) \bullet f(b)$ for any $a, b \in G$. Then D is also a group.

And one of G goes into one of D : $f(e_G) = e_D$ and for any $a \in G$: $f(a^{-1}) = f(a)^{-1}$.

Moreover, if G is commutative then D is also commutative.

Proof. Let $\tilde{a}, \tilde{b}, \tilde{c}$ are any elements of D , each of these elements has can be uniquely represented as $\tilde{a} = f(a)$, $\tilde{b} = f(b)$, $\tilde{c} = f(c)$ where $a, b, c \in G$. Then

$$(\tilde{a} \bullet \tilde{b}) \bullet \tilde{c} = (f(a) \bullet f(b)) \bullet f(c) = f(a \cdot b) \bullet f(c) = f((a \cdot b) \cdot c) = f(a \cdot (b \cdot c)) = f(a) \bullet f(b \cdot c) = f(a) \bullet (f(b) \bullet f(c)) = \tilde{a} \bullet (\tilde{b} \bullet \tilde{c}),$$

then the associative law is true in $[D, \bullet]$. Let's show that $f(e_G)$ is a “one” of D . For any $\tilde{a} \in D$ let's

consider $\tilde{a} \bullet f(e_G) = f(a) \bullet f(e_G) = f(a \cdot e_G) = f(a) = \tilde{a}$ and similarly $f(e_G) \bullet \tilde{a} = \tilde{a}$,

therefore $f(e_G) = e_D$. Let's finally show that for any element of D there exist an inverse one.

We fix an arbitrary $\tilde{a} \in D$, then $\tilde{a} = f(a)$. Let's show that the element $f(a^{-1})$ is an inverse to \tilde{a} .

So $\tilde{a} \bullet f(a^{-1}) = f(a) \bullet f(a^{-1}) = f(a \cdot a^{-1}) = f(e_G) = e_D$ and similarly $f(a^{-1}) \bullet \tilde{a} = e_D$.

Now we can say that D is a group. We have already shown that $f(e_G) = e_D$, and by the way,

in the process we have also shown that $f(a^{-1}) = f(a)^{-1}$. Really, the element $f(a^{-1})$ is an inverse to $\tilde{a} = f(a)$, it means exactly that $f(a^{-1}) = f(a)^{-1}$.

Let now G is a commutative group. Let's fix arbitrary elements $\tilde{a}, \tilde{b} \in D$, then $\tilde{a} \bullet \tilde{b} = f(a) \bullet f(b) = f(a \cdot b) = f(b \cdot a) = f(b) \bullet f(a) = \tilde{b} \bullet \tilde{a}$, then D is also a commutative group.

We can rewrite this [lemma](#) for additive groups: $(G, +)$ is an additive group and $[D, \oplus]$ is some set with a binary operation " \oplus ": $D \times D \rightarrow D$ on it. If there exist one-to-one mapping $f: G \rightarrow D$ such that $f(a + b) = f(a) \oplus f(b)$ for any $a, b \in G$, then D is also a group.

And zero of G goes into zero of D : $f(0_G) = 0_D$ and for any $a \in G$: $f(-a) = -f(a)$.

Moreover, if G is commutative, then D is also commutative.

Let's prove now [the theorem4](#): Let $f: R \rightarrow D$ is one-to-one correspondence with the properties $f(a + b) = f(a) \oplus f(b)$ and $f(a \cdot b) = f(a) \bullet f(b)$ for any $a, b \in R$. Let R is a ring, then $(R, +)$ is a commutative group with respect to the addition "+", and (D, \oplus) is a set with the binary operation \oplus , as $f: R \rightarrow D$ is one-to-one mapping and $f(a + b) = f(a) \oplus f(b)$, then (by [lemma6](#)) (D, \oplus) is a commutative group with respect to \oplus . As f is one-to-one and $f(a \cdot b) = f(a) \bullet f(b)$, then f conserves the associative law for multiplication: $\forall \tilde{a}, \tilde{b}, \tilde{c} \in D: (\tilde{a} \bullet \tilde{b}) \bullet \tilde{c} = \tilde{a} \bullet (\tilde{b} \bullet \tilde{c})$ (the proof is exactly the same as in the [lemma6](#)). And let's finally show that the distributive law is true in D , then we will be able to say that D is a ring. For any $\tilde{a}, \tilde{b}, \tilde{c} \in D$:

$$(\tilde{a} \oplus \tilde{b}) \bullet \tilde{c} = (f(a) \oplus f(b)) \bullet f(c) = f(a + b) \bullet f(c) = f((a + b) \cdot c) = f(a \cdot c + b \cdot c) = f(a \cdot c) \oplus f(b \cdot c) = (f(a) \bullet f(c)) \oplus (f(b) \bullet f(c)) = \tilde{a} \bullet \tilde{c} \oplus \tilde{b} \bullet \tilde{c}.$$

And similarly $\tilde{c} \bullet (\tilde{a} \oplus \tilde{b}) = \tilde{c} \bullet \tilde{a} \oplus \tilde{c} \bullet \tilde{b}$. Therefore, if R is a ring, then D is a ring.

Let R is a field, the mapping f transfers zero 0_R into zero 0_D (because f is one-to-one mapping of additive groups $(R, +) \xrightarrow{f} (D, \oplus)$). Let's discard zeroes from the sets R and D , then f is still one-to-one mapping $f: (R \setminus \{0_R\}) \rightarrow (D \setminus \{0_D\})$. As $((R \setminus \{0_R\}), \cdot)$ is a commutative multiplicative group and $(D \setminus \{0_D\}, \bullet)$ is a set with a binary operation \bullet on it, from the condition $f(a \cdot b) = f(a) \bullet f(b)$, by [lemma6](#), we get that $(D \setminus \{0_D\}, \bullet)$ is also a commutative multiplicative group $\Rightarrow D$ is a field.

Complement [for theorem4]. If $(R, +, \cdot)$ is a (commutative ring)/(ring with one), then $[D, \oplus, \bullet]$ is also a (commutative ring)/(ring with one).

Ordered rings and fields

Def: a ring/field $(R, +, \cdot)$ is called an ordered ring/field if there exist some subset $M \subset R$ of elements, that we will call “positive”, (so $a \in M \Leftrightarrow a$ is “positive”) and

[A] for any $a \in R$ exactly one of the next cases is true: a is positive, **or** $-a$ is positive, **or** $a = 0$.

[B] If a, b are positive, then $a + b$ and $a \cdot b$ are positive.

Notice. From **[A]** follows that $0 \notin M$. In practice when we have some ring/field $(R, +, \cdot)$ we need to mark some set $M \subset R$, which is closed with respect to addition and multiplication and does not contain a zero element 0 , such that: for any $a \in R$ only one of the next cases is true:

$a \in M$, **or** $-a \in M$, **or** $a = 0$.

Any ordered ring/field $(R, +, \cdot)$ must be always turned into an ordered set, the order “ $>$ ” must be defined in the next way.

Def. For any elements $a, b \in R$ we define: $a > b$ if $(a - b) \in M$ **and** $b > a$ if $(b - a) \in M$.

Correctness. “ $>$ ” is an order relation on R .

Proof. We need to show that any elements $a, b \in R$ are comparable and also that “ $>$ ” is transitive, then R is an ordered set by definition. Let’s fix any $a, b \in R$ and consider the element $(a - b)$.

According to **[B]**, only one of the next cases is true: $(a - b) \in M$, **or** $(-(a - b) \in M \Leftrightarrow (b - a) \in M)$, **or** $(a - b) = 0$ it is equivalent to $a > b$, **or** $b > a$, **or** $a = b$, then any $a, b \in R$ are comparable.

We also have to show that the relation “ $>$ ” is transitive: (if $a > b$ and $b > c$, then $a > c$).

Let $a > b$ and $b > c$, then $(a - b) \in M$ and $(b - c) \in M$. The set M is closed with respect to addition, then $(a - b) + (b - c) = (a - c) \in M \Rightarrow a > c$, then “ $>$ ” is transitive. So “ $>$ ” is an order relation on M .

Def. Any element $a \in R$ such that $-a \in M$ is called “negative”. So, any element $a \in R$ is positive, or negative, or zero.

Properties of ordered rings/fields.

Property1. R is an ordered ring/field.

Then: a is positive $\Leftrightarrow a > 0$. And: a is negative $\Leftrightarrow a < 0$.

Proof: Let a is positive $\Rightarrow a \in M \Rightarrow (a - 0) \in M \Rightarrow a > 0$.

Conversely: $a > 0 \Rightarrow (a - 0) \in M \Rightarrow a \in M$ then a is positive.

Next: a is negative $\Rightarrow -a \in M \Rightarrow (0 - a) \in M \Rightarrow 0 > a \Leftrightarrow a < 0$.

And similarly: $a < 0 \Rightarrow a$ is negative.

Property2 [sign rules]. R is an ordered ring. Then for any $a > 0, b > 0 \Rightarrow a + b > 0, a \cdot b > 0$, if R is a field, then also $a/b > 0$. In any ord. ring R : if $a < 0, b < 0 \Rightarrow a + b < 0, a \cdot b > 0$, if R is also a field, then also $a/b > 0$. In any ord. ring R : if $a > 0, b < 0$, or $a < 0, b > 0$, then $a \cdot b < 0$, if R is also a field, then also $a/b < 0$ and $b/a < 0$.

Remember that when R is just a ring, division ":" is not defined on R , we can speak about division only when R is a field.

Property3. Any ordered ring does not have any zero divisors.

Proof: R is an ordered ring. Let $a \cdot b = 0$, but $a \neq 0, b \neq 0$.

If $a > 0, b > 0 \Rightarrow$ / property 2 / $\Rightarrow a \cdot b > 0 \Rightarrow a \cdot b \neq 0$.

If $a < 0, b < 0 \Rightarrow$ / property 2 / $\Rightarrow a \cdot b > 0 \Rightarrow a \cdot b \neq 0$. If $a > 0, b < 0$ or $a < 0, b > 0$, then $a \cdot b < 0 \Rightarrow a \cdot b \neq 0$. So in any case $a \cdot b \neq 0$ and there are no zero divisors in R .

Absolute value

Def. R is an ordered ring/field and $a \in R$. The absolute value of a is the element $|a| \in R$ such that: if $a = 0$, then $|a| = 0$, if $a > 0$, then $|a| = a$, if $a < 0$, then $|a| = -a$.

In each case it's enough to consider separately all the variants. In the case [A] $a > 0$ and $a < 0$. For [B],[C] we consider separately each case: $a > 0, b > 0$ and $a < 0, b < 0$ and $a > 0, b < 0$ and $a < 0, b > 0$. Let's notice that in the case [C] it's enough to prove that $|a + b| \leq |a| + |b|$, then $|a| = |(a + b) + (-b)| \leq |a + b| + |-b| = |a + b| + |b|$. Then $|a| \leq |a + b| + |b| \Rightarrow |a| - |b| \leq |a + b|$.

Def. R is an ordered ring/field. We say that the **Archimedes axiom** is true in R if for any positive elements $a, b \in R$ there exist the natural number n such that $n \cdot a > b$.

Property4. R is an ordered ring/field.

[A] $a > b \Leftrightarrow -a < -b$ [B] $a + c > b + c$ (for some $c \in R$) $\Rightarrow a > b$. And $a > b \Rightarrow a + c > b + c$ (for any $c \in R$).

[C] $a \cdot c > b \cdot c$ (for some $c > 0$) $\Rightarrow a > b$. And $a > b \Rightarrow a \cdot c > b \cdot c$ (for any $c > 0$).
 $a \cdot c > b \cdot c$ (for some $c < 0$) $\Rightarrow a < b$. And $a < b \Rightarrow a \cdot c > b \cdot c$ (for any $c < 0$).

[D] $a > b, c > d \Rightarrow a + c > b + d$

Property5. R is an ordered field (use [C] from the property4).

[A] $b \cdot d > 0$, then: $\frac{a}{b} > \frac{c}{d} \Leftrightarrow a \cdot d > c \cdot b$ [B] $b \cdot d < 0$, then: $\frac{a}{b} > \frac{c}{d} \Leftrightarrow a \cdot d < c \cdot b$

Exercise: In any ordered ring/field $a \neq 0 \Rightarrow a^2 > 0$.

Theorem5 [Transfer of order]. Suppose we have exactly the same conditions as in the **theorem4**.

Then: If $(R, +, \cdot)$ is an ordered ring/field, then $[D, \oplus, \bullet]$ is also an ordered ring/field.

And f is one-to-one correspondence between positive and negative elements of these rings/fields:

a is positive/negative (in R) $\Leftrightarrow f(a)$ is positive/negative (in D).

And f conserves the order relation: $a < b$ (in R) $\Leftrightarrow f(a) < f(b)$ (in D).

Proof. Let M is a set of “positive elements” in R , i.e., M is a set with the properties **[A]** and **[B]** (from the definition above). Let's show that $f(M) \equiv \{f(m) \mid m \in M\}$ is the a with the same properties in D . From **[A]** follows that R is divided into the next sets without common elements $R = -M \cup \{0_R\} \cup M$, as $f : R \rightarrow D$ is one-to-one, then D is divided into the next sets without common elements: $D = f(-M) \cup f(0_R) \cup f(M)$. We know that f is an isomorphism of additive groups $(R, +) \rightarrow (D, +)$, then $f(0_R) = 0_D$ and also $f(-a) = -f(a)$ for any $a \in R$.

Then for any set $X \subset R$: $f(-X) = -f(X)$ and in particular $f(-M) = -f(M)$.

Then $D = -f(M) \cup \{0_D\} \cup f(M)$ (the sets on the right side do not have any common elements).

Then the condition **[A]** is true for $f(M) \subset D$, i.e., for any $d \in D$ exactly one of the next cases is true: $d \in f(M)$, $d = 0_D$, $d \in -f(M) \Leftrightarrow -d \in f(M)$. Also $f(M)$ is closed under

addition \oplus /multiplication \bullet , because M is closed under addition $+$ /multiplication \cdot .

Then the condition **[B]** is true for $f(M)$. **Therefore** D is an ordered ring/field and the positive elements $f(M) \subset D$ are exactly the images of the positive elements $M \subset R$.

Then: a is positive in $R \Leftrightarrow f(a)$ is positive in D . Similarly, the negative elements $-f(M) \subset D$ are exactly the images of the negative elements $-M \subset R$.

Then: a is negative in $R \Leftrightarrow f(a)$ is negative in D .

Next. Let $a < b$ in R , then $(b - a)$ is positive in R , then $f(b - a)$ is positive in D .

Let's simplify: $f(b - a) = f(b + (-a)) = f(b) \oplus f(-a) = f(b) \oplus (-f(a)) = f(b) - f(a)$ - this element is positive in D , then $f(a) < f(b)$ in D .

Conversely. Let $f(a) < f(b)$ in D . Then $f(b) - f(a) = f(b - a)$ is positive in D , then $b - a$ is positive in R , then $b > a$ in R . Everything is proved.

Exercise6. R is an ordered ring/field. Then any **nonzero** subring/subfield $H \subset R$ is also an ordered ring/field. And $\forall a, b \in H : a < b \text{ (in } H) \Leftrightarrow a < b \text{ (in } R)$.

Notice, when we say “nonzero subring” we mean $H \neq \{0\}$. Really, the set $H = \{0\}$ is a subring of R which consists of only zero element. The word “nonzero” above refers to “subring”, because $H = \{0\}$ is not a field, so there can’t be any zero subfield.

Solution. Let’s take the set of positive elements $M \subset R$ and consider the set $M \cap H$.

This set is not empty. Really, as $H \neq \{0\}$, then there exist $a \in H \parallel a \neq 0$. Then (according to the properties of the set $M \subset R$) either $a \in M$, or $-a \in M$. In the same time both $a \in H, -a \in H$ (because H is a ring). Then $M \cap H$ contains a or $-a$. So $M \cap H$ is not empty.

Let’s define: the set $M \cap H$ is the set of positive elements in H . Let’s check the main requirements:

[A] For any $a \in H$ only one of the next cases is true: $a \in M \cap H$, or $-a \in M \cap H$, or $a = 0$.

Let’s take any $a \in H$. If $a = 0 \in H$, then $a \notin M \cap H$ and $-a \notin M \cap H$ (because $0 \notin M$).

Let $a \neq 0 \in H$. We will show that there can be only one of the next cases:

$a \in M \cap H$, or $-a \in M \cap H$. As a is an element of the ring R , then $a \in M$, or $-a \in M$.

[1-st variant] $a \in M$, then $-a \notin M$. Also $a \in H$ and $-a \in H$. Then $a \in M \cap H$

and $-a \notin M \cap H$. **[2-nd variant]** $-a \in M$, then $a \notin M$. Also $-a \in H$ and $a \in H$.

Then $-a \in M \cap H$ and $a \notin M \cap H$.

[B] If a, b are positive (belong to $M \cap H$), then $a + b$ and $a \cdot b$ are positive (belong to $M \cap H$).

Really, let $a, b \in M \cap H$, then $a, b \in M$ (both a, b are positive in R), then $a + b, a \cdot b \in M$.

Next, $a, b \in H$, then (H is a ring) $a + b, a \cdot b \in H$. So $a + b, a \cdot b \in M \cap H$. We have proved that any subring/subfield $H \subset R$ is also an ordered ring/field. And $M \cap H$ are exactly the positive elements of H , where M are the positive elements of R .

Let’s fix now any $a, b \in H$. Let $a < b \text{ (in } H)$, then $(b - a)$ is positive in H

$\Leftrightarrow (b - a) \in M \cap H \Rightarrow (b - a) \in M$, then $(b - a)$ is positive in R , so $a < b \text{ (in } R)$.

Let now $a, b \in H$ and $a < b \text{ (in } R)$, then $(b - a) \in M$. Also $(b - a) \in H$ (because H is a ring),

then $(b - a) \in M \cap H$, so $(b - a)$ is positive in H , then $a < b \text{ (in } H)$. Everything is proved.

3

Matrixes

Matrixes

Everywhere later Ω is a set with addition and multiplication on it (binary operations on Ω) which both associative, commutative and these operations are connected by the distributive law. For example, $\Omega = \mathbb{N}$, or Ω is a commutative ring, or Ω is a field. Each of these variants is appropriate.

Def. Any table with m rows and n columns, which is formed from some elements of Ω , is called an $m \times n$ matrix (or just a matrix).

For example, $\begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 3 & 8 \end{pmatrix}$ and $\begin{pmatrix} 3 & 4 \\ 5 & 8 \end{pmatrix}$ are all 2×2 matrixes (here we use the set $\Omega = \mathbb{N}$).

And $(3 \ 1 \ 5)$ is 1×3 matrix, $\begin{pmatrix} 1 & 2 & 4 \\ 3 & 5 & 5 \end{pmatrix}$ is 2×3 matrix. By definition, any 1×1 matrix (a) is exactly the element a , so $(a) \equiv a$. When the number of rows m and the number of columns n are equal: $m = n$, we say that we have “a square matrix”. When $m \neq n$ we say that we have “a rectangular matrix”.

The element of a matrix A which stays at the intersection of the row with number i and the column with number j is denoted like a_{ij} .

For example: $A = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$, then $a_{11} = 1$, $a_{21} = 2$, $a_{12} = 3$, $a_{22} = 4$.

In general, $m \times n$ matrix A can be denoted as: $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$.

Matrixes A and B are equal ($A = B$) if they have exactly the same size ($m_A = m_B, n_A = n_B$) and they consist of the same elements $a_{ij} = b_{ij} \ \forall i, j$.

Def. Let A and B are both $m \times n$ matrixes (of the same size), then their sum is $m \times n$ matrix C such that $c_{ij} = a_{ij} + b_{ij} \ \forall i, j$. And we denote $A + B = C$.

For example, $\begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} + \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \equiv \begin{pmatrix} 1+3 & 3+2 \\ 2+1 & 1+4 \end{pmatrix} = \begin{pmatrix} 4 & 5 \\ 3 & 5 \end{pmatrix}$ and $(1 \ 2) + (2 \ 3) \equiv (1+2 \ 2+3) = (3 \ 5)$.

Addition of matrixes is commutative and associative: $A + B = B + A$ and $(A + B) + C = (A + B) + C$ for any $m \times n$ matrixes A, B, C (because addition on Ω is commutative and associative).

Def. The product of any $1 \times n$ matrix $A = (a_{11}, a_{12} \dots a_{1n})$ and any $n \times 1$ matrix $B = \begin{pmatrix} b_{11} \\ b_{21} \\ \dots \\ b_{n1} \end{pmatrix}$ is 1×1

matrix (the number) $a_{11} \cdot b_{11} + a_{12} \cdot b_{21} + \dots + a_{1n} \cdot b_{n1}$. So, by definition:

$$(a_{11} \quad a_{12} \quad \dots \quad a_{1n}) \cdot \begin{pmatrix} b_{11} \\ b_{21} \\ \dots \\ b_{n1} \end{pmatrix} = a_{11} \cdot b_{11} + a_{12} \cdot b_{21} + \dots + a_{1n} \cdot b_{n1}.$$

For example, $(1 \quad 2) \cdot \begin{pmatrix} 3 \\ 1 \end{pmatrix} = 1 \cdot 3 + 2 \cdot 1 = 5$ and $(3 \quad 1 \quad 1) \cdot \begin{pmatrix} 1 \\ 3 \\ 2 \end{pmatrix} = 3 \cdot 1 + 1 \cdot 3 + 1 \cdot 2 = 8.$

We have defined how to multiply a row and a column (any $1 \times n$ row and any $n \times 1$ column).

We can also multiply matrixes of appropriate sizes (only if the number of columns in A is equal to the number of rows in B , then the product (matrix) $A \cdot B$ is defined).

Def. Let A is $m \times n$ and B is $n \times k$ matrix (notice that the number n of columns in A and the number n of rows in B are equal). The product $A \cdot B$ is $m \times k$ matrix C such that: every element $c_{ij} \in C$ (the element at the intersection of i -th row and j -th column) is a product of i -th row of A and j -th column of B .

Suppose that we need to calculate $A \cdot B$. Let's take the first row of A , we will multiply this row consecutively by the 1-st, 2-nd, 3-rd... columns of B , the results of these multiplications must be placed at the first row of $A \cdot B$. Then we take the second row of A , and we multiply it consecutively by the 1-st, 2-nd, 3-rd... columns of B , the results must be placed at the second row of $A \cdot B$ and etc.

By definition, for any element $c_{ij} \in C = A \cdot B$ we have:

$$c_{ij} \equiv (i\text{-th row of } A) \cdot \begin{pmatrix} j\text{-th} \\ \text{column} \\ \text{of} \\ B \end{pmatrix} = (a_{i1} \quad a_{i2} \quad \dots \quad a_{in}) \cdot \begin{pmatrix} b_{1j} \\ b_{2j} \\ \dots \\ b_{nj} \end{pmatrix} = a_{i1} \cdot b_{1j} + a_{i2} \cdot b_{2j} + \dots + a_{in} \cdot b_{nj}$$

For example, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ is 2×3 matrix and $\begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}$ is a 3×1 matrix, so they can be multiplied:

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 2 \cdot 2 + 3 \cdot 1 \\ 3 \cdot 1 + 2 \cdot 2 + 1 \cdot 1 \end{pmatrix} = \begin{pmatrix} 8 \\ 8 \end{pmatrix}.$$

Let's take 3×3 matrix $\begin{pmatrix} 5 & 3 & 1 \\ 2 & 3 & 2 \\ 7 & 1 & 1 \end{pmatrix}$ and 3×1 matrix $\begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}$, these matrixes can be multiplied:

$$\begin{pmatrix} 5 & 3 & 1 \\ 2 & 3 & 2 \\ 7 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 5 \cdot 1 + 3 \cdot 1 + 1 \cdot 2 \\ 2 \cdot 1 + 3 \cdot 1 + 2 \cdot 2 \\ 7 \cdot 1 + 1 \cdot 1 + 1 \cdot 2 \end{pmatrix} = \begin{pmatrix} 10 \\ 9 \\ 10 \end{pmatrix}.$$

Let's take $A = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 3 \end{pmatrix}$. We can multiply these matrixes, because their sizes are 2×1

and 1×2 , so $A \cdot B = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 & 1 \cdot 3 \\ 2 \cdot 1 & 2 \cdot 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix}$, here we can also calculate

$$B \cdot A = \begin{pmatrix} 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} = 1 \cdot 1 + 3 \cdot 2 = 7.$$

It's always very easy to calculate the size of a product-matrix: if A is $m \times n$ and B is $n \times k$, then $A \cdot B$ is $m \times k$.

Multiplication of matrixes is NOT commutative. Really, let A is 3×1 and B is 1×2 matrix, then $A \cdot B$ is defined and $B \cdot A$ is not even defined. Both matrixes $A \cdot B$ and $B \cdot A$ are defined only when B and A have sizes $m \times n$ and $n \times m$. And if $m \neq n$, then $A \cdot B$ and $B \cdot A$ are matrixes of different sizes, so they can't be equal. Only when $m = n$ (when A and B are both square $n \times n$ matrixes) matrixes $A \cdot B$ and $B \cdot A$ have the same size $n \times n$. But even in this case we can't guarantee that these matrixes are equal.

Associativity. Multiplication of matrixes is associative: $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ for any matrixes A, B, C .

Remark. In order the product $A \cdot (B \cdot C)$ to be defined, the matrixes must have appropriate sizes: $A \leftrightarrow m \times n$, $B \leftrightarrow n \times k$, $C \leftrightarrow k \times h$. In this way, both products $A \cdot (B \cdot C)$ and $(A \cdot B) \cdot C$ are defined. And obviously $A \cdot (B \cdot C)$ and $(A \cdot B) \cdot C$ are both matrixes of the same size $m \times h$.

Proof. Let's show that every element ω_{ij} of $A \cdot (B \cdot C)$ is equal to the element θ_{ij} of $(A \cdot B) \cdot C$.

Let's fix any element ω_{ij} of $A \cdot (B \cdot C)$, then:

$$\omega_{ij} = (\text{the row with number } i \text{ of } A) \times (\text{the column with number } j \text{ of } B \cdot C) = (a_{i1}, a_{i2} \dots a_{in}) \bullet \begin{pmatrix} p_{1j} \\ p_{2j} \\ \dots \\ p_{nj} \end{pmatrix}.$$

The column with number j of $B \cdot C$ consists of the elements:

$$\begin{pmatrix} p_{1j} \\ p_{2j} \\ \dots \\ p_{nj} \end{pmatrix} = \begin{pmatrix} (\text{the row with number 1 of } B) \times (\text{the column with number } j \text{ of } C) \\ (\text{the row with number 2 of } B) \times (\text{the column with number } j \text{ of } C) \\ \dots \\ (\text{the row with number } n \text{ of } B) \times (\text{the column with number } j \text{ of } C) \end{pmatrix} = \begin{pmatrix} \sum_{1 \leq s \leq k} b_{1s} \cdot c_{sj} \\ \sum_{1 \leq s \leq k} b_{2s} \cdot c_{sj} \\ \dots \\ \sum_{1 \leq s \leq k} b_{ns} \cdot c_{sj} \end{pmatrix}$$

$$\Rightarrow \omega_{ij} = (a_{i1}, a_{i2} \dots a_{in}) \cdot \begin{pmatrix} \sum_{1 \leq s \leq k} b_{1s} \cdot c_{sj} \\ \sum_{1 \leq s \leq k} b_{2s} \cdot c_{sj} \\ \dots \\ \sum_{1 \leq s \leq k} b_{ns} \cdot c_{sj} \end{pmatrix} = a_{i1} \cdot \left(\sum_{1 \leq s \leq k} b_{1s} \cdot c_{sj} \right) + a_{i2} \cdot \left(\sum_{1 \leq s \leq k} b_{2s} \cdot c_{sj} \right) + \dots + a_{in} \cdot \left(\sum_{1 \leq s \leq k} b_{ns} \cdot c_{sj} \right) =$$

$$= a_{i1} \cdot (b_{11}c_{1j} + b_{12}c_{2j} + \dots + b_{1k}c_{kj}) + a_{i2} \cdot (b_{21}c_{1j} + b_{22}c_{2j} + \dots + b_{2k}c_{kj}) + \dots \\ \dots + a_{in} \cdot (b_{n1}c_{1j} + b_{n2}c_{2j} + \dots + b_{nk}c_{kj})$$

Let's regroup our summands, we want the numbers $c_{1j}, c_{2j} \dots c_{kj}$ to be in front of the brackets:

$$= c_{1j} \cdot (a_{i1}b_{11} + a_{i2}b_{21} + \dots + a_{in}b_{n1}) + c_{2j} \cdot (a_{i1}b_{12} + a_{i2}b_{22} + \dots + a_{in}b_{n2}) + \dots \\ \dots + c_{kj} \cdot (a_{i1}b_{1k} + a_{i2}b_{2k} + \dots + a_{in}b_{nk}) \equiv \omega_{ij} \quad [1].$$

Let's calculate the element θ_{ij} of $(A \cdot B) \cdot C$:

$$\theta_{ij} = (\text{the row with number } i \text{ of } A \cdot B) \times (\text{the column with number } j \text{ of } C) = (z_{i1}, z_{i2} \dots z_{ik}) \bullet \begin{pmatrix} c_{1j} \\ c_{2j} \\ \dots \\ c_{kj} \end{pmatrix}$$

The row with number i of $A \cdot B$ consists of the elements:

$$\begin{aligned}
 & (z_{i1}, z_{i2} \dots z_{ik}) = \\
 & = \left((i - \text{th row of } A) \times (1 - \text{st column of } B) \dots (i - \text{th row of } A) \times (k - \text{th column of } B) \right) = \\
 & = \left((a_{i1}, a_{i2} \dots a_{in}) \bullet \begin{pmatrix} b_{11} \\ b_{21} \\ \dots \\ b_{n1} \end{pmatrix} \quad (a_{i1}, a_{i2} \dots a_{in}) \bullet \begin{pmatrix} b_{12} \\ b_{22} \\ \dots \\ b_{n2} \end{pmatrix} \quad , \dots , \quad (a_{i1}, a_{i2} \dots a_{in}) \bullet \begin{pmatrix} b_{1k} \\ b_{2k} \\ \dots \\ b_{nk} \end{pmatrix} \right) = \\
 & = \left(\sum_{1 \leq s \leq n} a_{is} \cdot b_{s1}, \sum_{1 \leq s \leq n} a_{is} \cdot b_{s2} \dots \sum_{1 \leq s \leq n} a_{is} \cdot b_{sk} \right) \Rightarrow \text{then } \theta_{ij} = \left(\sum_{1 \leq s \leq n} a_{is} \cdot b_{s1}, \sum_{1 \leq s \leq n} a_{is} \cdot b_{s2} \dots \sum_{1 \leq s \leq n} a_{is} \cdot b_{sk} \right) \bullet \begin{pmatrix} c_{1j} \\ c_{2j} \\ \dots \\ c_{kj} \end{pmatrix} \\
 & = c_{1j} \cdot \left(\sum_{1 \leq s \leq n} a_{is} \cdot b_{s1} \right) + c_{2j} \cdot \left(\sum_{1 \leq s \leq n} a_{is} \cdot b_{s2} \right) \dots + c_{kj} \cdot \left(\sum_{1 \leq s \leq n} a_{is} \cdot b_{sk} \right) = \\
 & = c_{1j} \cdot (a_{i1}b_{11} + a_{i2}b_{21} + \dots + a_{in}b_{n1}) + c_{2j} \cdot (a_{i1}b_{12} + a_{i2}b_{22} + \dots + a_{in}b_{n2}) + \dots \\
 & \dots + c_{kj} \cdot (a_{i1}b_{1k} + a_{i2}b_{2k} + \dots + a_{in}b_{nk}) \equiv \theta_{ij} \quad [2].
 \end{aligned}$$

Let's compare [1] and [2], we see that $\omega_{ij} = \theta_{ij}$, it proves that $A \cdot (B \cdot C) = (A \cdot B) \cdot C$.

As multiplication of matrixes is associative, then in any product of several matrixes we can rearrange brackets in any way we want, it will not change the result of multiplication.

For example, $(A \cdot B) \cdot (C \cdot D) \cdot (E \cdot F) = A \cdot ((B \cdot C) \cdot D \cdot (E \cdot F))$.

It's very easy to prove the distributive law for matrix-multiplication.

[A] $(A + B) \cdot C = A \cdot C + B \cdot C$ (for any $m \times n$ matrixes A, B and any $n \times k$ matrix C),

[B] $C \cdot (A + B) = C \cdot A + C \cdot B$ (for any $m \times n$ matrix C and any $n \times k$ matrixes A and B).

Def. For any element $\lambda \in F$ and any $m \times n$ matrix A . The matrix $\lambda \cdot A$ is such matrix C that $c_{ij} = \lambda \cdot a_{ij} \forall i, j$.

$$\text{For example: } 2 \cdot \begin{pmatrix} 1 & 4 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} 2 & 8 \\ 6 & 10 \end{pmatrix} \text{ and } 2 \cdot (3 \ 2 \ 4) = (6 \ 4 \ 8).$$

Let's consider the set M of all $m \times n$ matrixes which elements are taken from some commutative ring R . It's easy to see that M is a commutative additive group. Really, addition of matrixes is commutative and associative, the zero matrix O is $m \times n$ matrix which consists of zeroes.

For any $m \times n$ matrix A , an opposite matrix $-A$ is the matrix which consists of opposite elements: $A = \{a_{ij}\} \Rightarrow -A \equiv \{-a_{ij}\}$. So M is a commutative group.

Then we can speak about subtraction "-" on M . For any matrixes $A, B \in M$, their difference is the matrix $C \in M$ such that $A = B + C$. We can consider the last equality as an equation $A = B + C$, where A, B are fixed matrixes, and we have to find the matrix C .

As $A = B + C \Leftrightarrow a_{ij} = b_{ij} + c_{ij} \parallel \forall i, j \Rightarrow c_{ij} = a_{ij} - b_{ij} \parallel \forall i, j$.

Then: for any $m \times n$ matrixes A and B , their difference $(A - B)$ is the matrix C such that $c_{ij} = a_{ij} - b_{ij} \forall i, j$.

For example, $\begin{pmatrix} 3 & 9 \\ 5 & 8 \end{pmatrix} - \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 6 \\ 4 & 4 \end{pmatrix}$ and $(5 \ 5 \ 5) - (3 \ 2 \ 1) = (2 \ 3 \ 4)$.

If we consider the set $M^{n \times n}$ of all square $n \times n$ matrixes. Then $M^{n \times n}$ is a ring.

Really, $M^{n \times n}$ is obviously a commutative group under addition. Multiplication (on $M^{n \times n}$) is associative and distributive over addition. So $M^{n \times n}$ is a ring. Let's notice that $M^{n \times n}$ mustn't be a field, at least because the multiplication of square matrixes (in general) is not commutative.

Def: a square $n \times n$ matrix A is called symmetric if it has a symmetry with respect to it's main diagonal $a_{11}, a_{22}, \dots, a_{nn}$. We can write it shortly: A is symmetric if $a_{ij} = a_{ji} \forall i, j$.

For such matrix any i -th row of A and i -th column of A consist of the same elements.

From here immediately follows the next simple fact: multiplication of symmetric matrixes is commutative, i.e., for any symmetric matrixes A, B we have $A \cdot B = B \cdot A$ (understand why).



4

*Integer
numbers*

Integer numbers

Def. \mathbb{Z} is the ring that consists of natural numbers $\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$, the zero number 0 , and all the numbers that are opposite to naturals $\mathbb{N} \equiv \{-1, -2, -3, -4, -5, \dots\}$, so $\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}$.

The addition and multiplication on \mathbb{Z} are extensions of the addition and multiplication on \mathbb{N} , i.e., for any $a, b \in \mathbb{N} \subset \mathbb{Z}$: $a + b$ (addition by the rules of \mathbb{Z}) $= a + b$ (addition by the rules of \mathbb{N}), $a \cdot b$ (multiplication by the rules of \mathbb{Z}) $= a \cdot b$ (multiplication by the rules of \mathbb{N}).

The ring \mathbb{Z} is called a ring of integer numbers and elements of \mathbb{Z} are called integer numbers.

Let's build \mathbb{Z} . We fix any set \mathbb{N} of natural numbers. Let's consider the set Ω of all pairs $\{(a, b)\}$ where a, b are any natural numbers. Let's define addition and multiplication on Ω .

Def. $(a, b) \oplus (c, d) \equiv \text{by def} \equiv (a + c, b + d)$ and $(a, b) \bullet (c, d) \equiv \text{by def} \equiv (a \cdot c + b \cdot d, a \cdot d + b \cdot c)$

How to remember it? Imagine that any pair (a, b) denotes the difference $a - b$ of elements a, b in some ring, then $(a, b) \oplus (c, d) \leftrightarrow (a - b) + (c - d) = (a + c) - (b + d) \leftrightarrow (a + c, b + d)$ and $(a, b) \bullet (c, d) \leftrightarrow (a - b) \cdot (c - d) = (a \cdot c + b \cdot d) - (a \cdot d + b \cdot c) \leftrightarrow (a \cdot c + b \cdot d, a \cdot d + b \cdot c)$.

For any pair (a, b) , its elements are natural numbers a, b . And we have already learned all the basic properties of natural numbers (the addition and multiplication of natural numbers are commutative and associative, there is also a distributive law and etc.).

Assertion 1. The addition " \oplus " and multiplication " \bullet " (of pairs) are both commutative and associative on Ω . There is also a distributive law:

$$((a, b) \oplus (c, d)) \bullet (e, m) \approx ((a, b) \bullet (e, m)) \oplus ((c, d) \bullet (e, m)) \text{ and } (e, m) \bullet ((a, b) \oplus (c, d)) \approx ((e, m) \bullet (a, b)) \oplus ((e, m) \bullet (c, d)).$$

Proof. We could check all these properties straightly. Let's give a more interesting proof.

We consider the set X of all 2×2 symmetric matrixes of natural numbers.

$X \equiv \left\{ A = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{N} \right\}$ - this set is closed under the matrix addition and multiplication, really:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} + \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} a + c & b + d \\ b + d & a + c \end{pmatrix} \text{ and } \begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} a \cdot c + b \cdot d & a \cdot d + b \cdot c \\ b \cdot c + a \cdot d & b \cdot d + a \cdot c \end{pmatrix}.$$

Let's define the mapping $f : X \rightarrow \Omega$: for any matrix $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ its image is the pair (a, b) ,

so $f \left(\begin{pmatrix} a & b \\ b & a \end{pmatrix} \right) \equiv (a, b)$. Then f is one-to-one mapping, and f obviously has the next properties

[T] $\forall A, B \in X: f(A + B) = f(A) \oplus f(B)$, $f(A \cdot B) = f(A) \bullet f(B)$ (so f is a "sort of" isomorphism).

All the properties, that are listed in the [assertion 1](#), are true on X (because X consists of 2×2

symmetric matrixes, and all the properties from the [assertion1](#) are the standard properties of square matrixes, except commutativity of multiplication, but it is true for any symmetric matrixes of the same size). And we have one-to-one mapping $f : X \rightarrow \Omega$ such that [T].

Then f transfers all the needed properties (associativity/commutativity/distributivity of addition/multiplication) **from** X **to** Ω and the [assertion1](#) is proved.

Comment: we have showed the transition of all these properties in the [theorem4](#) ("Groups, rings, fields"). The proof was done for rings/fields, and the Reader could notice that X is not a ring/field. Now the situation is more simple, because X has just some properties of a ring (but not all of them), and because of [T], f transfers all these properties from X to Ω .

Let's define the equivalence relation " \approx " on the set Ω of all pairs. By definition, pairs (a,b) and (c,d) are equivalent $(a,b) \approx (c,d)$ if $a + d = b + c$. It's very easy to see that " \approx " is really an equivalence relation on Ω , because it is reflexive, symmetric and transitive. Therefore this relation divides Ω into the classes $A, B, C, D, E \dots$ of equivalent pairs. All pairs in any class are equivalent to each other. And the classes $A, B, C, D, E \dots$ do not have any common elements (common pairs). The set of all classes we denote like Z_{aux} (aux=auxiliary).

Let's define addition and multiplication on Z_{aux} in order to turn Z_{aux} into a ring.

Def. Let A, B are any classes from Z_{aux} . And $(a,b) \in A$, $(c,d) \in B$ are any pairs from these classes. The sum $A \oplus B$ is the class that contains the sum of pairs (a,b) and (c,d) , i.e., the pair $(a + c, b + d) = (a,b) \oplus (c,d)$. The product $A \bullet B$ is the class that contains the product of pairs (a,b) and (c,d) , i.e., the pair $(a \cdot c + b \cdot d, a \cdot d + b \cdot c) = (a,b) \bullet (c,d)$.

Notice: we use the same symbols \oplus and \bullet to denote the addition and multiplication of classes, as we used for the addition and multiplication of pairs. But of course, the addition/multiplication of pairs and classes are different operations which are defined on different sets. But there is no need to complicate our designations, let's just stick to \oplus and \bullet .

Assertion2. The given definition is correct. For any classes $A, B \in Z_{aux}$, a sum $A \oplus B$ and a product $A \bullet B$ are uniquely defined (it doesn't matter which pairs (a,b) and (c,d) are chosen from A and B).

Proof. Let $(a,b), (\bar{a}, \bar{b}) \in A$ and $(c,d), (\bar{c}, \bar{d}) \in B$. We just need to show that

$(a,b) \oplus (c,d) \approx (\bar{a}, \bar{b}) \oplus (\bar{c}, \bar{d})$ and $(a,b) \bullet (c,d) \approx (\bar{a}, \bar{b}) \bullet (\bar{c}, \bar{d})$, then the classes $A \oplus B$ and

$A \bullet B$ are uniquely defined. As $(a,b), (\bar{a}, \bar{b}) \in A$, then $a + \bar{b} = \bar{a} + b$, as $(c,d) \approx (\bar{c}, \bar{d})$, then

$c + \bar{d} = \bar{c} + d$. Let's sum two last equalities:

$$(a + \bar{b}) + (c + \bar{d}) = (\bar{a} + b) + (\bar{c} + d) \Rightarrow (a + c) + (\bar{b} + \bar{d}) = (\bar{a} + \bar{c}) + (b + d) \text{ [T].}$$

By definition, $(a, b) \oplus (c, d) = (a + c, b + d)$ and $(\bar{a}, \bar{b}) \oplus (\bar{c}, \bar{d}) = (\bar{a} + \bar{c}, \bar{b} + \bar{d})$.

From [T] we see that pairs $(a + c, b + d)$ and $(\bar{a} + \bar{c}, \bar{b} + \bar{d})$ are equivalent, therefore:

$$(a, b) \oplus (c, d) \approx (\bar{a}, \bar{b}) \oplus (\bar{c}, \bar{d}).$$

The “straight proof” here is inconvenient, let’s prove the auxiliary equivalence: if $(a, b) \approx (\bar{a}, \bar{b})$, then for any pair (c, d) there must be: $(a, b) \bullet (c, d) \approx (\bar{a}, \bar{b}) \bullet (c, d)$ [aux].

We have the basic equality: $a + \bar{b} = \bar{a} + b$ [D]. So $(a, b) \bullet (c, d) \approx (a \cdot c + b \cdot d, a \cdot d + b \cdot c)$ and $(\bar{a}, \bar{b}) \bullet (c, d) = (\bar{a} \cdot c + \bar{b} \cdot d, \bar{a} \cdot d + \bar{b} \cdot c)$. We need to show that

$(a \cdot c + b \cdot d, a \cdot d + b \cdot c) \approx (\bar{a} \cdot c + \bar{b} \cdot d, \bar{a} \cdot d + \bar{b} \cdot c)$ it is equivalent to:

$(a \cdot c + b \cdot d) + (\bar{a} \cdot d + \bar{b} \cdot c) = (\bar{a} \cdot c + \bar{b} \cdot d) + (a \cdot d + b \cdot c)$ and this equality is equivalent to:

$(a + \bar{b}) \cdot c + (b + \bar{a}) \cdot d = (\bar{a} + b) \cdot c + (\bar{b} + a) \cdot d$ [V], let’s check that it is true by using [D].

We can substitute everywhere (in [V]) $a + \bar{b}$ instead of $\bar{a} + b$. Then [V] looks like

$(a + \bar{b}) \cdot c + (a + \bar{b}) \cdot d = (a + \bar{b}) \cdot c + (a + \bar{b}) \cdot d$ - which is a true equality, then [aux] is proved.

Let’s prove now the main one, as $(a, b) \approx (\bar{a}, \bar{b})$, then $(a, b) \bullet (c, d) \approx (\bar{a}, \bar{b}) \bullet (c, d)$.

As $(c, d) \approx (\bar{c}, \bar{d})$, then $(\bar{a}, \bar{b}) \bullet (c, d) \approx (\bar{a}, \bar{b}) \bullet (\bar{c}, \bar{d})$ and therefore $(a, b) \bullet (c, d) \approx (\bar{a}, \bar{b}) \bullet (\bar{c}, \bar{d})$.

Assertion3. The set $(Z_{aux}, \oplus, \bullet)$ (of all classes) is a commutative ring with one.

Proof. The addition of pairs is commutative and associative, therefore the addition of classes is also commutative and associative. The zero O is the class which contains $(1, 1)$. Really, for any class A , the class $A + O$ is the class which contains $(a, b) \oplus (1, 1) \parallel (a, b) \in A, (1, 1) \in O$.

Then $A + O$ contains $(a + 1, b + 1)$. But the pair $(a + 1, b + 1)$ is equivalent to (a, b) , because $(a + 1) + b = (b + 1) + a$ therefore $A \oplus O = A$ and similarly $O \oplus A = A$.

So O is a zero element of Z_{aux} . Next, for any class A which contains (a, b) , an opposite class $-A$ is the class which contains (b, a) . Really, let’s fix an arbitrary $(a, b) \in A$. The pair (b, a) belongs to some class B . Then $A \oplus B$ contains the pair $(a, b) \oplus (b, a) = (a + b, b + a) \approx (1, 1)$. Therefore

$A \oplus B = O$ and similarly $B \oplus A = O$, then, by definition, B is an opposite to A element, so $B = -A$.

Therefore Z_{aux} is a commutative group under addition.

The multiplication of pairs is associative, then the multiplication of classes is also associative. And finally, there is a distributive law for pairs, from here immediately follows the distributive law for classes. Then Z_{aux} is a ring. Moreover, the multiplication of pairs is commutative, then the

multiplication of classes is also commutative, so Z_{aux} is a commutative ring. There is also the class “one” I which contains the pair $(2,1)$. Really, for any class A the class $A \bullet I$ contains the pair $(a,b) \bullet (2,1) \parallel (a,b) \in A, (2,1) \in I$. But $(a,b) \bullet (2,1) = (a \cdot 2 + b \cdot 1, a \cdot 1 + b \cdot 2)$ this pair is equivalent to (a,b) , then $A \bullet I = A$ and similarly $I \bullet A = A$. Then I is an element “one” of Z_{aux} .

Conclusion: Z_{aux} is a commutative ring with one.

Def: a class $A \in Z_{aux}$ is called **positive** if for any pair $(a,b) \in A$: $a > b$.

Correctness. The given definition is correct. If $a > b$ for some pair (a,b) , then $c > d$ for any pair $(c,d) \in A$.

Proof. Let $(a,b) \in A$ and $a > b$, let's take any other pair $(c,d) \in A$.

Then $(a,b) \approx (c,d) \Rightarrow a + d = c + b$.

If $c = d$, then from $a > b$ follows that $a + d > c + b$. If $c < d$, then from $a > b$ follows that $a + d > c + b$. Then, the only possible variant is $c > d$.

Conclusion. If $a > b$ for some pair from A , then the same is true for any other pair from A .

It's very easy to prove the similar assertion for the case $a < b$. And finally, if $a = b$ for some pair from A , then the same is true for any other pair and $A = O$.

We can sum up: for any class $A \in Z_{aux}$ only one of the next cases is true:

[E] A is positive, **or** $-A$ is positive, **or** $A = O$ (remember that if $(a,b) \in A$, then $(b,a) \in -A$).

Def. Let N_{POS} is the set of all positive classes of Z_{aux} .

Assertion4. Z_{aux} is an ordered ring.

Proof. For any class $A \in Z_{aux}$ **[E]** is true. According to the basic definition, besides **[E]**, we also need

to show that if A, B are positive, then both $A \oplus B$ and $A \bullet B$ are positive. Let's take any $(a,b) \in A \parallel a > b$ and $(c,d) \in B \parallel c > d$, then obviously, the pair $(a,b) \oplus (c,d) = (a+b, c+d)$ is a positive pair, and similarly $(a,b) \bullet (c,d) = (a \cdot c + b \cdot d, a \cdot d + b \cdot c)$ is positive, let's show the last one: $a > b \Rightarrow a = b + \Delta$ and $c > d \Rightarrow c = d + \delta$, then $a \cdot c + b \cdot d = (b + \Delta) \cdot (d + \delta) + b \cdot d = b \cdot d + b \cdot \delta + \Delta \cdot d + \Delta \cdot \delta + b \cdot d$ and $a \cdot d + b \cdot c = (b + \Delta) \cdot d + b \cdot (d + \delta) = b \cdot d + \Delta \cdot d + b \cdot d + b \cdot \delta$, we can compare two sums that we obtained, it's easy to see that $a \cdot c + b \cdot d > a \cdot d + b \cdot c$, and the pair $(a,b) \bullet (c,d)$ is positive.

From here immediately follows that $A \oplus B$ and $A \bullet B$ are positive classes.

We have shown that Z_{aux} is an ordered ring.

According to the rules of any ordered ring, the class $B \in Z_{aux}$ is called negative if $-B$ is positive.

Let $(a,b) \in B$, then $(b,a) \in -B$, if $-B$ is positive, then $b > a$. Then for any pair (a,b) from any

negative class B we have $a < b$. Let N_{NEG} is the set of all negative classes. As any class of the ring Z_{aux} is positive, or negative, or zero, then $Z_{aux} = N_{NEG} \cup O \cup N_{POS}$.

Assertion5.

For any positive class $A \in N_{POS}$ there exist the unique natural number Δ such that

$$\forall (a,b) \in A: a = b + \Delta.$$

And for any natural number Δ there exist the unique positive class A such that

$$\forall (a,b) \in A: a = b + \Delta.$$

For any negative class $B \in N_{NEG}$ there exist the unique natural number Δ such that

$$\forall (a,b) \in B: a + \Delta = b.$$

And for any natural number Δ there exist the unique negative class B such that

$$\forall (a,b) \in B: a + \Delta = b.$$

Proof. Existence. Let A is a positive class: $\forall (a,b),(c,d) \in A: a + d = c + b$ it is an equality of natural numbers. Here $a > b$ and $c > d$, then both sides of the equality $a + d = c + b$ are greater than $(b + d)$, so we can subtract $(b + d)$ from both sides:

$$(a + d) - (b + d) = (c + b) - (b + d) \Rightarrow a - b = c - d.$$

So, for any pairs $(a,b),(c,d) \in A \Rightarrow a - b = c - d \equiv / \text{by def} / \equiv \Delta$.

Then $a = b + \Delta$ and $c = d + \Delta$ and similarly for any other pair from A .

Uniqueness. Let for some natural number Δ we have $\forall (a,b) \in A: a = b + \Delta$, and in the same time for the other natural number $\delta \neq \Delta$ we also have: $\forall (a,b) \in A: a = b + \delta$, then $b + \delta = b + \Delta \Rightarrow \delta = \Delta$.

Next. Existence. Let's fix any natural Δ and consider the class A which contains the pair $(1 + \Delta, 1)$, then A is positive. For any $(a,b) \in A$ we have $(a,b) \approx (1 + \Delta, 1)$, then $a + 1 = 1 + \Delta + b \Rightarrow a = b + \Delta$.

Uniqueness. Let for some natural number Δ we have the classes A, B such that $a = b + \Delta$ for any $(a,b) \in A$ and $c = d + \Delta$ for any $(c,d) \in B$. Let's sum the equalities we have in the next way: $a + (d + \Delta) = (b + \Delta) + c \Rightarrow a + d = b + c \Rightarrow (a,b) \approx (c,d) \Rightarrow A = B$.

For any negative class $B \in N_{NEG}$ the proof is similar.

Let's build now the set Z of integer numbers. We take Z_{aux} and every class A from N_{POS} with a pair $(a,b) \in A$ we replace by the natural number Δ such that $a = b + \Delta$ ([assertion5](#)).

Then instead every positive class we will have exactly one natural number. And the set N_{POS} will

turn into the set \mathbb{N} of natural numbers. All the other classes of Z_{aux} must stay untouched.

$Z \equiv \mathbb{N}_{NEG} \cup \mathbb{O} \cup \mathbb{N}_{POS} \rightarrow \mathbb{N}_{NEG} \cup \mathbb{O} \cup \mathbb{N} \equiv Z$. The set $Z \equiv \mathbb{N}_{NEG} \cup \mathbb{O} \cup \mathbb{N}$ is called a **set of integer numbers**. This set consists of natural numbers and classes of equivalent pairs (of natural numbers). We need to define addition and multiplication on Z (because Z consists of natural numbers and classes, and we don't know how to add or multiply those).

Def. Any elements $a, b \in Z$ have unique representations as $a = f(A)$, $b = f(B)$, where A, B are some classes of the ring Z_{aux} . Then we define $a + b = f(A) + f(B) \equiv /by\ def/ \equiv f(A \oplus B)$ and $a \cdot b = f(A) \cdot f(B) \equiv /by\ def/ \equiv f(A \bullet B)$.

Let's define one-to-one mapping $f : Z_{aux} \rightarrow Z$ such that

$$\begin{array}{ccc} \mathbb{N}_{NEG} & \mathbb{O} & \mathbb{N}_{POS} \\ \downarrow & \downarrow & \downarrow \\ \mathbb{N}_{NEG} & \mathbb{O} & \mathbb{N} \end{array} .$$

For any class $B \in (\mathbb{N}_{NEG} \cup \mathbb{O})$ we define $f(B) \equiv B$. For any class $A \in \mathbb{N}_{POS}$, which contains a pair $(a, b) : a = b + \Delta$, we define $f(A) \equiv \Delta$. Then f is one-to-one mapping.

Then the addition "+" and multiplication "." are binary operations on Z . And $(Z, +, \cdot)$ is a set with two binary operations on it. We see that: $f : Z_{aux} \rightarrow Z$ is one-to-one mapping such that $f(A \oplus B) = f(A) + f(B)$ and $f(A \bullet B) = f(A) \cdot f(B)$ for any $A, B \in Z_{aux}$.

From the **theorem4** (page 40) immediately follows that $(Z, +, \cdot)$ is a ring.

From the **complement for theorem4** follows that Z is a commutative ring and a ring with one. According to the **theorem5 (Transfer of order)** (page 44), Z is an ordered ring and natural numbers $\mathbb{N} \subset Z$ are the only positive elements of Z .

Property1. The addition and multiplication on Z are extensions of the addition and multiplication of natural numbers, i.e., for any $a, b \in \mathbb{N} \subset Z$ we have:

$$a + b \text{ (addition by the rules of } Z) = a + b \text{ (addition by the rules of } \mathbb{N}),$$

$$a \cdot b \text{ (multiplication by the rules of } Z) = a \cdot b \text{ (multiplication by the rules of } \mathbb{N})$$

And similarly, the order relation ">" on Z is an extension of the order relation on \mathbb{N} :

$$a > b \text{ (by the rules of } Z) = a > b \text{ (by the rules of } \mathbb{N}).$$

Proof. For illustration purposes, let's denote for a while $(\tilde{+}, \tilde{\cdot})$ - the addition and multiplication on the ring Z and $(+, \cdot)$ - the addition and multiplication on \mathbb{N} . Let's fix arbitrary natural numbers $a, b \in \mathbb{N} \subset Z$. In order to find the sum $a \tilde{+} b$ (in Z) we need to find the positive classes A, B (from Z_{aux}) such that $f(A) = a$, $f(B) = b$, then, by definition, $a \tilde{+} b = f(A) \tilde{+} f(B) \equiv f(A \oplus B)$.

So, A is the class with the pair $(1 + a, 1)$ and B is the class with the pair $(1 + b, 1)$.

The class $A \oplus B$ contains the pair $(1 + a, 1) \oplus (1 + b, 1) = ((1 + a) + (1 + b), 1 + 1) = (2 + (a + b), 2)$, then $f(A \oplus B) = (a + b)$ and therefore $a \tilde{+} b = a + b$ for any $a, b \in \mathbb{N}$.

Next, $a \tilde{\cdot} b = f(A) \tilde{\cdot} f(B) \equiv f(A \bullet B)$ and $(A \bullet B)$ is the class which contains the pair $(1 + a, 1) \bullet (1 + b, 1) = ((1 + a) \cdot (1 + b) + 1 \cdot 1, (1 + a) \cdot 1 + 1 \cdot (1 + b)) = ((2 + a + b) + a \cdot b, (2 + a + b))$ then $f(A \bullet B) = a \cdot b$ therefore $a \tilde{\cdot} b = a \cdot b \forall a, b \in \mathbb{N}$.

And finally, $a, b \in \mathbb{N}$ and $a \tilde{>} b$ (in \mathbb{Z}). The order relation on \mathbb{Z} was transferred from \mathbb{Z}_{aux} , so, $a \tilde{>} b \Leftrightarrow f(A) \tilde{>} f(B) \Leftrightarrow A > B$ (in \mathbb{Z}_{aux}) (look at the **theorem5 (Transfer of order)**).

So $a \tilde{>} b \Leftrightarrow A > B$ and the **assertion** $a \tilde{>} b$ (in \mathbb{Z}) $\Leftrightarrow a > b$ (in \mathbb{N}) (that we want to prove) is equivalent to $A > B$ (in \mathbb{Z}_{aux}) $\Leftrightarrow a > b$ (in \mathbb{N}). As $a = f(A)$, then A contains the pair $(1 + a, 1)$, as $b = f(B)$, then B contains the pair $(1 + b, 1)$. Let $A > B$ (in \mathbb{Z}_{aux}), it means that the class $(A - B) = A \oplus (-B)$ is positive in \mathbb{Z}_{aux} . The class $A \oplus (-B)$ contains the pair $(1 + a, 1) \oplus (1, 1 + b) = (2 + a, 2 + b)$ as $A \oplus (-B)$ is positive, then $2 + a > 2 + b \Rightarrow a > b$ (in \mathbb{N}).

Conversely. Let $a > b$ (in \mathbb{N}), then the class $(A - B) = A \oplus (-B)$ with the pair $(2 + a, 2 + b)$ is positive, then $A > B$ (in \mathbb{Z}_{aux}).

Conclusion: as the order relation/ addition/multiplication on \mathbb{Z} are all extensions of the order relation/ addition/multiplication on $\mathbb{N} \subset \mathbb{Z}$, then it's appropriate to use exactly the same signs ($< + \cdot$) (as we used on \mathbb{N}) to denote these operations on \mathbb{Z} .

Property2. The zero class $O \in \mathbb{Z}$ is a zero element of the ring \mathbb{Z} , so $O \equiv 0$.

For any negative class $B \in \mathbb{N}_{NEG}$ there exist the unique natural number $\Delta \in \mathbb{N} \subset \mathbb{Z}$ such that $B = -\Delta$. And finally: $\mathbb{Z} = -\mathbb{N} \cup O \cup \mathbb{N}$.

Proof. Let's fix any $a \in \mathbb{Z}$, it can be uniquely represented as $a = f(A)$.

Then $a + O = f(A) + f(O) = f(A \oplus O) = f(A) = a$ and similarly $O + a = a$, then O is a zero element of \mathbb{Z} . **Next,**

Existence. Let's fix any $B \in \mathbb{N}_{NEG}$. Then $B \in \mathbb{Z}_{aux}$. According to the **assertion5**,

there is the unique natural number Δ such that $\forall (a, b) \in B: a + \Delta = b$, and B contains the pair $(1, 1 + \Delta)$. The class $-B \in \mathbb{Z}_{aux}$ is the class that contains the pair $(1 + \Delta, 1)$.

Then $B \oplus (-B) = O$ (in Z_{aux}), therefore $f(B \oplus (-B)) = f(O) \Leftrightarrow f(B) + f(-B) = f(O)$.

Here $f(B) = B$ and $f(-B) = \Delta$ and $f(O) = O = 0$, then $B + \Delta = 0 \Rightarrow B = -\Delta$.

Uniqueness. Let $B = -\Delta$ and $B = -\delta$, where $\Delta, \delta \in \mathbb{N}$. Then $-\Delta = -\delta \Rightarrow \Delta = \delta$,

and the uniqueness is proved.

Let's finally show that $Z = -N \cup O \cup N$. We consider the set $N_{NEG} \subset Z$ and the set $-N \subset Z$.

Let's will show that $N_{NEG} = -N$. It's enough to show that $N_{NEG} \subset -N$ and $-N \subset N_{NEG}$

(then $-N = N_{NEG}$). Let's fix any class $B \in N_{NEG}$. As we showed above, there exist the unique natural number Δ such that $B = -\Delta \in -N \Leftrightarrow B \in -N$, then $N_{NEG} \subset -N$.

Conversely, let's fix now any element $-\delta \in -N$, then $\delta \in \mathbb{N}$.

Let's consider the class T with the pair $(1, 1 + \delta)$, as $1 < 1 + \delta$, then $T \in N_{NEG}$ and

$T + \delta = 0$ (in Z) $\Rightarrow -\delta = T \in N_{NEG} \Leftrightarrow -\delta \in N_{NEG}$, then $-N \subset N_{NEG}$.

As $N_{NEG} = -N$ and also $O \equiv 0$ and (according to our construction) $Z = N_{NEG} \cup O \cup N$, then $Z = -N \cup O \cup N$. The [property2](#) is proved.

Let's show that Z is a minimal ring which contains \mathbb{N} . Here we need to notice, that when we speak about some ring R which contains \mathbb{N} , we imply not only that $\mathbb{N} \subset R$, but also that addition and multiplication on R are extensions of the addition and multiplication on \mathbb{N} . If we do not make such requirement, the addition and multiplication on \mathbb{N} do not make any sense in R . And all the properties of natural numbers, which are connected with addition/multiplication/order, mustn't be true in R . In such case we can't say anything determined about R , except that it contains all the elements (symbols) of \mathbb{N} .

Property3. Z is a minimal ring which contains \mathbb{N} , it means that:
any other ring R , which contains \mathbb{N} , contains Z as a subring.

Let some ring R contains \mathbb{N} , this ring must also contain a zero element $0 \in R$ (and obviously 0 can't be an element of \mathbb{N} , because $\forall a \in \mathbb{N} : a + b > b$ for any $b \in \mathbb{N}$, so any $a \in \mathbb{N}$ can't be a zero element of R . Here we can see why we require from addition on R to be an extension of the addition on \mathbb{N}). The ring R must also contain all the elements which are opposite to natural numbers \mathbb{N} (because R is an additive group). And any element $-a$, which is opposite to a natural number a , can't belong to $\mathbb{N} \subset R$.

Really, $-a + a = 0$, if we assume that $-a \in \mathbb{N}$, then both $a, -a \in \mathbb{N}$ and therefore $0 \in \mathbb{N}$

(because a sum of natural numbers is a natural number), but $0 \notin \mathbb{N}$, so we have a contradiction.

We showed that $\{0\} \cap \mathbb{N} = \emptyset$ and $-\mathbb{N} \cap \mathbb{N} = \emptyset$. Let's finally show that $-\mathbb{N} \cap \{0\} = \emptyset$, if it's not true, then $0 \in -\mathbb{N}$, then $0 = -a$ for some $a \in \mathbb{N}$, then $a = 0$ which is not true. So, any two of the sets $-\mathbb{N}, \{0\}, \mathbb{N}$ do not intersect in R . Let's denote $\tilde{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}$, any element of \tilde{Z} is a natural number, or an opposite to some natural, or zero.

According to the rules that govern addition and multiplication in any ring, (like $-a - b = -(a + b)$, $a - b = a + (-b)$, $(-a) \cdot (-b) = a \cdot b$), sum/difference/product of any elements $a, b \in \tilde{Z}$ are again some elements of \tilde{Z} , then \tilde{Z} is a subring of R (subring criterion). Then \tilde{Z} is an independent ring, inside R . As addition/multiplication on R are extensions of the addition/multiplication on $N \subset R$, then addition/multiplication on \tilde{Z} are extensions of the addition/multiplication on $N \subset \tilde{Z}$. It's easy to see that \tilde{Z} is a ring of integer numbers (according to the initial definition). Everything is proved.

Uniqueness. We have built the ring of integer numbers Z , based on some set N of natural numbers that we have fixed at the very beginning. Formally, there exist different sets of natural numbers (of course, all of them are isomorphic as ordered sets), and formally, we can construct different sets Z . The main question that appears here: are these sets of integer numbers also isomorphic? And the answer is "Yes". All sets of integer numbers are isomorphic as rings. And we will show even more.

Uniqueness theorem. Any rings Z_A and Z_B of integer numbers are isomorphic. Moreover, the isomorphism $f : Z_A \rightarrow Z_B$ is unique, this isomorphism is an extension of the unique isomorphism $f : N_A \rightarrow N_B$ (look at [the theorem3/advanced theorem3](#) for natural numbers).

Proof: [[Existence](#)]. Let's build the isomorphism $f : Z_A \rightarrow Z_B$. We take the unique isomorphism $f : N_A \rightarrow N_B$. It's explicit definition is $f(1_A) \equiv 1_B$ and if $f(a_A) = a_B$, then $f(n(a_A)) \equiv n(a_B)$.

As we showed above: $Z = (-N) \cup 0 \cup N$, so

$$Z_A = (-N_A) \cup 0_A \cup N_A = \{\dots -3_A, -2_A, -1_A, 0_A, 1_A, 2_A, 3_A, \dots\} \text{ and}$$

$$Z_B = (-N_B) \cup 0_B \cup N_B = \{\dots -3_B, -2_B, -1_B, 0_B, 1_B, 2_B, 3_B, \dots\}.$$

$$\begin{array}{ccccccccc} \dots & -3_A & -2_A & -1_A & 0_A & 1_A & 2_A & 3_A & \dots \\ & & & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \end{array}$$

And f is one-to-one correspondence:

$$\begin{array}{ccccccccc} \dots & -3_B & -2_B & -1_B & 0_B & 1_B & 2_B & 3_B & \dots \end{array}$$

Let's extend f . We define $f(0_A) \equiv 0_B$, and for any negative number $-a_A \in -N_A$ we define $f(-a_A) \equiv -f(a_A)$.

$$\begin{array}{ccccccccc} \dots & -3_A & -2_A & -1_A & 0_A & 1_A & 2_A & 3_A & \dots \\ \text{Then } f \text{ becomes one-to-one mapping} & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \dots & -3_B & -2_B & -1_B & 0_B & 1_B & 2_B & 3_B & \dots \end{array}$$

Really, we already know that $f : N_A \rightarrow N_B$ is one-to-one, also $f(0_A) = 0_B$, then

$f : \{0_A\} \cup N_A \rightarrow \{0_B\} \cup N_B$ is one-to-one. Let's finally show that $(-N_A) \xrightarrow{f} (-N_B)$ is one-to-one (then $f : Z_A \rightarrow Z_B$ is one-to-one). By definition: $-a_A \in -N_A \Rightarrow f(-a_A) \equiv -f(a_A)$.

From here we see that f is defined on the set $-N_A$, and the values of f on $-N_A$ lie in the set $-N_B$. So f is a mapping: $(-N_A) \xrightarrow{f} (-N_B)$.

[A] f covers the set $-N_B$. Let's take any element $-a_B \in -N_B \Rightarrow a_B \in N_B$, then there exist the unique $a_A \in N_A$ such that $f(a_A) = a_B$. Let's consider the element $-a_A \in -N_A$, by definition $f(-a_A) \equiv -f(a_A) = -a_B$.

[B] f does not "glue together" elements of $-N_A$. Let $f(-a_A) = f(-b_A) \parallel -a_A \neq -b_A$, we can rewrite it $-f(a_A) = -f(b_A) \parallel -a_A \neq -b_A$. Then $f(a_A) = f(b_A) \parallel a_A \neq b_A$, then different natural numbers a_A and b_A are transferred into the same (natural) number $f(a_A) = f(b_A)$ which is impossible, because $f : N_A \rightarrow N_B$ is one-to-one, and we have a contradiction.

Then $(-N_A) \xrightarrow{f} (-N_B)$ is one-to-one.

Now we can claim that $f : Z_A \rightarrow Z_B$ is really one-to-one. Let's show that $f : Z_A \rightarrow Z_B$ is a ring isomorphism. So we need to show that $\forall a_A, b_A : f(a_A + b_A) = f(a_A) + f(b_A)$ and $f(a_A \cdot b_A) = f(a_A) \cdot f(b_A)$. Let's consider several possibilities:

[1-st case] One of the numbers a_A, b_A is a zero number. Multiplication and addition are commutative in both rings, and both equalities (that we want to prove) are symmetrical with respect to a_A, b_A , without loss of generality we can assume that $a_A = 0_A$.

Then $f(a_A + b_A) = f(0_A + b_A) = f(b_A) = 0_B + f(b_A) = f(a_A) + f(b_A)$ and $f(a_A \cdot b_A) = f(0_A \cdot b_A) = f(0_A) = 0_B = 0_B \cdot f(b_A) = f(0_A) \cdot f(b_A) = f(a_A) \cdot f(b_A)$.

[2-nd case] Both a_A, b_A are not zero numbers. There can be exactly 3 variants **[A],[B],[C]**.

[A] Both numbers a_A, b_A are natural. In this case the properties $f(a_A + b_A) = f(a_A) + f(b_A)$ and $f(a_A \cdot b_A) = f(a_A) \cdot f(b_A)$ have already been proved (**advanced theorem3** for natural numbers).

[B] Both numbers a_A, b_A are negative. Then $a_A = -\tilde{a}_A$, $b_A = -\tilde{b}_A$, where \tilde{a}_A and \tilde{b}_A are natural. In the next actions we will use the sign rules which are true in any ring, like $a + (-b) = a - b$ and $-a + (-b) = -a - b = -(a + b)$ and $(-a) \cdot (-b) = a \cdot b$ and etc. We will also use the case **[A]** (**properties** of f for natural numbers). So,

$$f(a_A + b_A) = f(-\tilde{a}_A + (-\tilde{b}_A)) = f(-(\tilde{a}_A + \tilde{b}_A)) = //(\tilde{a}_A + \tilde{b}_A) \in N_A // = -f(\tilde{a}_A + \tilde{b}_A) = -(f(\tilde{a}_A) + f(\tilde{b}_A)) = -f(\tilde{a}_A) - f(\tilde{b}_A) = -f(\tilde{a}_A) + (-f(\tilde{b}_A)) = f(-\tilde{a}_A) + f(-\tilde{b}_A) = f(a_A) + f(b_A).$$

$$\text{And } f(a_A \cdot b_A) = f((- \tilde{a}_A) \cdot (- \tilde{b}_A)) = f(\tilde{a}_A \cdot \tilde{b}_A) = // \tilde{a}_A, \tilde{b}_A \in N_A // = f(\tilde{a}_A) \cdot f(\tilde{b}_A) = (-f(\tilde{a}_A)) \cdot (-f(\tilde{b}_A)) = f(-\tilde{a}_A) \cdot f(-\tilde{b}_A) = f(a_A) \cdot f(b_A).$$

[C] One of the numbers a_A, b_A is positive and the other one is negative. Similarly, as in the

[1-st case], we can assume that a_A is negative and b_A is positive, then $a_A = -\tilde{a}_A$ where \tilde{a}_A is natural and b_A is natural. Let's prove the simple part:

$$f(a_A \cdot b_A) = f(-(\tilde{a}_A) \cdot b_A) = f(-(\tilde{a}_A \cdot b_A)) = //(\tilde{a}_A \cdot b_A) \in N_A // = -f(\tilde{a}_A \cdot b_A) = -f(\tilde{a}_A) \cdot f(b_A) = f(-\tilde{a}_A) \cdot f(b_A) = f(a_A) \cdot f(b_A).$$

Let's consider now $f(a_A + b_A) = f((- \tilde{a}_A) + b_A) = f(b_A - \tilde{a}_A) \parallel \tilde{b}_A, \tilde{a}_A \in N$ here can be several

simple cases, in each case we will work with the expression $f(b_A - \tilde{a}_A)$

(which is equal to $f(a_A + b_A)$).

[C1] $b_A - \tilde{a}_A$ is natural, then $b_A - \tilde{a}_A = x_A \in N_A \Rightarrow b_A = \tilde{a}_A + x_A$, then $f(b_A - \tilde{a}_A) = f(x_A)$.

Let's consider now the sum

$f(a_A) + f(b_A) = f(-\tilde{a}_A) + f(\tilde{a}_A + x_A) = -f(\tilde{a}_A) + f(\tilde{a}_A) + f(x_A) = f(x_A)$. So, we have deduced that $f(a_A + b_A) = f(x_A)$ and $f(a_A) + f(b_A) = f(x_A)$.

[C2] $b_A - \tilde{a}_A = 0_A$, then $b_A = \tilde{a}_A$. Then $f(b_A - \tilde{a}_A) = f(0_A) = 0_B$.

Let's consider the sum $f(a_A) + f(b_A) = f(-\tilde{a}_A) + f(\tilde{a}_A) = -f(\tilde{a}_A) + f(\tilde{a}_A) = 0_B$.

And we have shown that $f(a_A + b_A) = 0_B$ and $f(a_A) + f(b_A) = 0_B$.

[C3] $b_A - \tilde{a}_A$ is a negative number, then $b_A - \tilde{a}_A = -x_A \parallel x_A \in N_A \Rightarrow b_A + x_A = \tilde{a}_A$.

Then $f(b_A - \tilde{a}_A) = f(-x_A) = /x_A \in N_A / = -f(x_A)$. Let's consider

$f(a_A) + f(b_A) = f(-\tilde{a}_A) + f(b_A) = -f(\tilde{a}_A) + f(b_A) = -f(b_A + x_A) + f(b_A) = //b_A, x_A \in N_A // = -(f(b_A) + f(x_A)) + f(b_A) = -f(x_A)$. And we have shown that $f(a_A + b_A) = -f(x_A)$ and $f(a_A) + f(b_A) = -f(x_A)$.

Everything is proved. $f : Z_A \rightarrow Z_B$ is a ring isomorphism.

Uniqueness. We have already built $f : Z_A \rightarrow Z_B$ which is an extension of the unique isomorphism $f : N_A \rightarrow N_B$. Let's show that if $\varphi : Z_A \rightarrow Z_B$ is a ring isomorphism, then $\varphi \equiv f$ on Z_A .

Let's assume that there exist some other ring-isomorphism $\varphi : Z_A \rightarrow Z_B$. As any isomorphism, φ must transfer zero into zero and one into one: $\varphi(0_A) = 0_B$ and $\varphi(1_A) = 1_B$. In the **main theorem** (for natural numbers) we have shown that every natural number $a_A \in N_A$ is a descendant of one $a_A = n(n(...(n(n(e_A))))))$, then a_A can be represented as a "sum of ones"

$a_A = n(n(...(n(n(e_A)))))) = n(n(...(n(e_A + e_A)))) = n(n(...(e_A + e_A + e_A))) = ... = e_A + e_A + ... + e_A$.

Then for any natural

$a_A \in N_A : \varphi(e_A + e_A + ... + e_A) = //\varphi(a + b) = \varphi(a) + \varphi(b)// = \varphi(e_A) + \varphi(e_A) + ... + \varphi(e_A) = e_B + e_B + ... + e_B \in N_B$, from here follows that the values of φ on the set N_A belong to the set N_B .

Then we can write $\varphi : N_A \rightarrow N_B$. Let's show that φ satisfies the conditions: $\varphi(1_A) = 1_B$ and if $\varphi(a_A) = a_B$, then $\varphi(n(a_A)) \equiv n(a_B)$.

If these conditions are true, then φ coincides with f on N_A . As we mentioned above, $\varphi(1_A) = 1_B$.

And if $\varphi(a_A) = a_B$, then $\varphi(n(a_A)) = \varphi(a_A + 1_A) = \varphi(a_A) + \varphi(1_A) = a_B + e_B = n(a_B)$. So $\varphi \equiv f$ on N_A .

As we mentioned earlier $\varphi(0_A) = 0_B$, then $\varphi \equiv f$ on $\{0_A\} \cup N_A$. The mapping f is defined on $(-N_A)$ by the rule $\forall -a_A \in -N_A \Rightarrow f(-a_A) \equiv -f(a_A)$. Let's fix an arbitrary $-a_A \in -N_A$.

According to the basic properties of any ring-isomorphism: $\varphi(-a_A) = -\varphi(a_A) \forall -a_A \in Z_A$ and in particular for any $-a_A \in N_A : \varphi(-a_A) = -\varphi(a_A) = //\varphi(a_A) = f(a_A)// = -f(a_A) = f(-a_A)$, then $\varphi \equiv f$ on $(-N_A)$. Then $\varphi \equiv f$ on Z_A .

Let's list the other simple, but very important properties of integer numbers.

Property4. The **Archimedes axiom** is true in \mathbb{Z} : for any positive $a, b \in \mathbb{Z}$ there exist the natural $n \in \mathbb{N}$ such that $n \cdot a > b$.

Proof. Let's fix arbitrary positive $a, b \in \mathbb{Z}$, then both $a, b \in \mathbb{N}$. And we have already proved the **Archimedes axiom** for \mathbb{N} .

Property5. Let X is a nonempty subset of \mathbb{Z} .

[A] If there exist some number M which is greater than any element of X , then X has the greatest number M_{\max} .

[B] If there exist some number m which is less than any element of X , then X has the least number m_{\min} .

Proof. **[A]** If there are some positive numbers in X , then these numbers are natural and there is a nonempty subset $N_X \subset X$ of natural numbers. If there exist some number M such that $x < M \parallel \forall x \in X \Rightarrow x < M \parallel \forall x \in N_X$ then (as we proved earlier) there exist the greatest number $M_{\max} \in N_X$, obviously M_{\max} is the greatest number in X .

If there are no positive numbers in X and $0 \in X$, then 0 is the greatest number in X .

Let there are no positive numbers in X and $0 \notin X$. Then there are only negative numbers in X , therefore $-X$ consists only of natural numbers, and (as we proved earlier) $-X$ has the least number $m_{\min} \in -X \parallel m_{\min} \leq -x \parallel \forall (-x) \in -X$, then $-m_{\min} \in X \parallel -m_{\min} \geq x \parallel \forall x \in X$ and $-m_{\min}$ is the greatest number in X .

The case **[B]**. There exist $m \leq x \parallel \forall x \in X$. We can simplify the proof if we consider the set $-X$ of integer numbers, then $-m \geq (-x) \parallel \forall (-x) \in -X$. So, the number $-m$ is greater than any number of $-X$. Let's use the result **[A]**, the set $-X$ contains the greatest number M_{\max} , then $-M_{\max}$ is the least number of X .

Divisibility

Def. $a, b \in \mathbb{Z}$ if there exist $k \in \mathbb{Z}$ such that $a = k \cdot b$, then we say “ a is divisible by b ” and we write $a : b$. Also when $a = k \cdot b$, we can say “ b divides a ”, or “ b is a divisor of a ” and we can write $b \mid a$.

Exercise: If $a, b \in \mathbb{N}$ and a is divisible by b , then $a \geq b$.

If $a, b \in \mathbb{Z} \parallel a \neq 0$ and a is divisible by b , then $|a| \geq |b|$.

Theorem1 [division with a remainder].

[1-st part] For any natural numbers a, b there exist the unique pair of integer numbers $k, r \parallel k \geq 0, 0 \leq r < b$ such that $a = k \cdot b + r$.

Proof: [A] Existence of numbers k, r . Let's fix arbitrary $a, b \in \mathbb{N}$, according to the **Archimedes axiom**, $\exists n \in \mathbb{N} : a < nb$. Let M is the set of all integer numbers m , for which $m \cdot b \leq a$.

Then $\forall m \in M : m \leq n$. Then there exist the greatest number $m_{\max} \in M$, obviously $m_{\max} \geq 0$

and obviously $m_{\max} \cdot b \leq a < (m_{\max} + 1) \cdot b$. Let's designate $k \equiv m_{\max}$, so we can write:

$k \cdot b \leq a < (k + 1) \cdot b$. Let's define $r \equiv a - k \cdot b$, then obviously $0 \leq r$. Let's show that $r < b$. If $r \geq b$, then $a - k \cdot b \geq b \Rightarrow a \geq (k + 1) \cdot b$ it contradicts to $a < (k + 1) \cdot b$, then $r < b$ and finally $0 \leq r < b$.

[B] Uniqueness of numbers k, r . Let's assume that there exist some other pair of integer numbers \bar{k}, \bar{r} which satisfies to the same conditions. Then $a = k \cdot b + r$ and $a = \bar{k} \cdot b + \bar{r}$, then

$k \cdot b + r = \bar{k} \cdot b + \bar{r}$. From the last equality follows that: if $k = \bar{k}$, then $\bar{r} = r$ and the uniqueness is proved. Let $k \neq \bar{k}$, without loss of generality $k > \bar{k}$. The equality $k \cdot b + r = \bar{k} \cdot b + \bar{r}$ is equivalent

to $(k - \bar{k}) \cdot b = \bar{r} - r$, here $(k - \bar{k}) \in \mathbb{N} \Rightarrow (k - \bar{k}) \geq 1 \Rightarrow (k - \bar{k}) \cdot b \geq b$. Also $0 \leq \bar{r} < b$ and

$0 \leq r < b \Rightarrow 0 \geq -r > -b \Leftrightarrow -b < -r \leq 0$ let's sum the last equality with $0 \leq \bar{r} < b$, then

$-b < \bar{r} - r < b$. So, the left part of the equality $(k - \bar{k}) \cdot b = \bar{r} - r$ is greater than or equal to b ,

and the right part is less than b , therefore $(k - \bar{k}) \cdot b > \bar{r} - r$, and we have a contradiction.

Then $k = \bar{k}$ and $\bar{r} = r$.

[2-nd part] For any integer numbers $a, b \in \mathbb{Z} \parallel b \neq 0$ there exist the unique pair of integer numbers $k, r \parallel 0 \leq r < |b|$ such that $a = k \cdot b + r$. And k is called a quotient of a, b .

r is called a remainder of a divided by b .

Proof. Existence of representation. If $a = 0$ let's take $k = 0, r = 0$. Let $a \neq 0$, then can be the next cases: [A] If $a > 0, b > 0$, then a, b are natural, everything is proved in this case.

[B] $a > 0, b < 0$. Let's take the natural numbers $a, (-b)$, then, according to the [1-st part]), there exist the representation: $a = \bar{k} \cdot (-b) + \bar{r} \parallel \bar{k} \geq 0, 0 \leq \bar{r} < (-b)$. As $b < 0$, then $(-b) = |b|$ and we can

rewrite $a = (-\bar{k}) \cdot b + \bar{r} \parallel (-\bar{k}) \in \mathbb{Z}, 0 \leq \bar{r} < |b|$. Now we just have to designate $k \equiv (-\bar{k})$ and $r \equiv \bar{r}$

and we have the representation we need: $a = k \cdot b + r \parallel k \in \mathbb{Z}, 0 \leq r < |b|$.

[C] $a < 0, b > 0$, or [D] $a < 0, b < 0$, both cases must be considered exactly as the case [B], by using the needed representation for natural numbers we get the similar representation for integers.

Uniqueness of representation. Let $a = k \cdot b + r$ and $a = \bar{k} \cdot b + \bar{r}$. Again, if $k = \bar{k}$, then $\bar{r} = r$ and the representation is unique. If $k \neq \bar{k}$, we will get the exactly similar contradiction, as we got earlier (in the uniqueness for natural numbers).

Decimal notation

Reminder. We have introduced earlier the natural numbers 1, 2, 3, ..., 10, and the set \mathbb{N} can be written like: $\mathbb{N} \equiv \{1, 2, 3, \dots, 10, n(n(n(n(n(n(n(n(n(1))))))))))\dots\}$.

Lemma1. For any natural number k the next equality is true:

$$9 \cdot 10^k + 9 \cdot 10^{k-1} + \dots + 9 \cdot 10^1 + 10 = 10^{k+1}.$$

Proof (by induction). When $k = 1$ we need to check: $9 \cdot 10^1 + 10 = 10^2$, let's simplify the left part, by using the distributive law: $(9 + 1) \cdot 10 = 10 \cdot 10 = 10^2$ - it is a true equality.

If the equality is true for a natural number k , then let's consider

$$\begin{aligned} 9 \cdot 10^{k+1} + 9 \cdot 10^k + 9 \cdot 10^{k-1} + \dots + 9 \cdot 10^1 + 10 &= 9 \cdot 10^{k+1} + (9 \cdot 10^k + 9 \cdot 10^{k-1} + \dots + 9 \cdot 10^1 + 10) = \\ 9 \cdot 10^{k+1} + 10^{k+1} &= (9 + 1) \cdot 10^{k+1} = 10 \cdot 10^{k+1} = 10^{k+2} \end{aligned}$$

and the equality is true for $k + 1 = n(k)$, then the equality is true for every natural number k .

Lemma2. For any natural $k \in \mathbb{N}$ there exist some $n \in \mathbb{N}$ such that $10^n \leq 10 + k < 10^{n+1}$.

Proof. Let $k = 1$, then $n = 1$ is appropriate, really $10 \leq 10 + 1$. Let's check that $10 + 1 < 10^{1+1}$ - it is equivalent to $1 < 10^2 - 10 \Leftrightarrow 1 < 10 \cdot (10 - 1) \Leftrightarrow 1 < 10 \cdot 9 \Leftrightarrow 1 \cdot 1 < 10 \cdot 9$, the last equality is true, because $1 < 9$, $1 < 10$. If our assertion is true for a natural number k , then let's consider it for

$(k + 1)$. As the assertion is true for k , then $10^n \leq 10 + k < 10^{n+1}$ for some $n \in \mathbb{N}$. As $10 + k < 10^{n+1}$ there can be the next cases: **[A]** If $10 + k = 10^{n+1} - 1$, then $10 + (k + 1) = 10^{n+1}$ and $10^{n+1} = 10 + (k + 1) < 10^{n+2} \Rightarrow 10^{n+1} \leq 10 + (k + 1) < 10^{n+2}$.

[B] If $10 + k \neq 10^{n+1} - 1$, then $10 + k < 10^{n+1} - 1$, then $10 + (k + 1) < 10^{n+1}$ and also $10^n \leq 10 + k < 10 + (k + 1)$, therefore $10^n \leq 10 + (k + 1) < 10^{n+1}$.

Our assertion is true for $(k + 1) \in \mathbb{N}$, therefore it is true for any natural number k .

The main theorem. For any $a \in \mathbb{N} \parallel a > 10$ there exist the unique representation as the sum:

$$a = \partial_n 10^n + \partial_{n-1} 10^{n-1} + \dots + \partial_1 10 + \partial_0, \text{ where } \partial_n, \partial_{n-1} \dots \partial_1, \partial_0 \text{ are integer numbers:}$$

$$1 \leq \partial_n \leq 9, 0 \leq \partial_{n-1} \leq 9, \dots, 0 \leq \partial_0 \leq 9.$$

[Existence of representation]. As $a > 10$, then $a = 10 + k$, where $k \in \mathbb{N}$.

Assertion. For any natural number $10 + k \parallel k \in \mathbb{N}$ there exist the representation from the main theorem. Let $k = 1$, then $10 + 1 = 1 \cdot 10 + 1 \parallel \partial_1 = 1, \partial_0 = 1$. Let our assertion is true for some numbers $1, 2, \dots, k$. Let's consider the number $10 + (k + 1)$. The number $10 + k$ can be represented as:

$$10 + k = \partial_n 10^n + \partial_{n-1} 10^{n-1} + \dots + \partial_1 10 + \partial_0, \text{ then } 10 + (k + 1) = \partial_n 10^n + \partial_{n-1} 10^{n-1} + \dots + \partial_1 10 + \partial_0 + 1.$$

[A] If $0 \leq \partial_0 \leq 8$, then $1 \leq (\partial_0 + 1) \leq 9$ and we can designate $\bar{\partial}_0 \equiv (\partial_0 + 1)$, then

$$10 + (k + 1) = \partial_n 10^n + \partial_{n-1} 10^{n-1} + \dots + \partial_1 10 + \bar{\partial}_0, \text{ it is the representation we need.}$$

[B] If $\partial_0 = 9$, then there can be the next cases:

[B1] All the other numbers $\partial_1, \partial_2 \dots \partial_m \dots \partial_n$ (from the representation for $10 + k$) are all equal to 9,

then $10 + k = 9 \cdot 10^n + 9 \cdot 10^{n-1} + \dots + 9 \cdot 10 + 9$, then

$$10 + (k + 1) = 9 \cdot 10^n + 9 \cdot 10^{n-1} + \dots + 9 \cdot 10 + 9 + 1 =$$

$$9 \cdot 10^n + 9 \cdot 10^{n-1} + \dots + 9 \cdot 10 + 10 = /lemma\ 7/ = 10^{n+1}.$$

Then $10 + (k + 1) = 1 \cdot 10^{n+1} + 0 \cdot 10^n + \dots + 0 \cdot 10 + 0 \parallel \partial_{n+1} = 1, \partial_n = 0 \dots \partial_0 = 0$ - it is the representation we need for $10 + (k + 1)$.

[B2] $\partial_0 = 9$ and maybe several numbers $\partial_1, \partial_2 \dots \partial_m$ (from the representation for $(10 + k)$) are **all** equal to 9, but $\partial_{m+1} \neq 9 \Rightarrow 0 \leq \partial_{m+1} \leq 8$.

Then $(10 + k) = \partial_n 10^n + \dots + \partial_{m+1} 10^{m+1} + 9 \cdot 10^m + 9 \cdot 10^{m-1} \dots + 9 \cdot 10 + 9$ and therefore

$$10 + (k + 1) = \partial_n 10^n + \dots + \partial_{m+1} 10^{m+1} + 9 \cdot 10^m + 9 \cdot 10^{m-1} \dots + 9 \cdot 10 + 9 + 1 = /lemma\ 7/ =$$

$$= \partial_n 10^n + \dots + \partial_{m+1} 10^{m+1} + 10^{m+1} = \partial_n 10^n + \dots + (\partial_{m+1} + 1) 10^{m+1}, \text{ then}$$

$$10 + (k + 1) = \partial_n 10^n + \dots + (\partial_{m+1} + 1) 10^{m+1}, \text{ where } 1 \leq (\partial_{m+1} + 1) \leq 9. \text{ Let's designate}$$

$$\bar{\partial}_{m+1} = (\partial_{m+1} + 1), \text{ then } 10 + (k + 1) = \partial_n 10^n + \dots + \bar{\partial}_{m+1} 10^{m+1} \text{ and the representation we need for}$$

$$10 + (k + 1) = \partial_n 10^n + \dots + \bar{\partial}_{m+1} 10^{m+1} + 0 \cdot 10^m + \dots + 0 \cdot 10 + 0.$$

Then for any natural number $a = 10 + k \parallel k \in \mathbb{N}$ there exist the representation from the **main theorem**. The existence is proved.

[Uniqueness of representation]. For any natural number a the representation (from above):

$$a = \partial_n 10^n + \partial_{n-1} 10^{n-1} + \dots + \partial_1 10 + \partial_0 \text{ is unique.}$$

Lemma3. There is a sum $b + c + d + \dots + m$. If every summand in the sum is divisible by $k \in \mathbb{N}$, then all the sum is also divisible by k .

Proof. As every summand is divisible by k , then $b = \bar{b} \cdot k, c = \bar{c} \cdot k \dots m = \bar{m} \cdot k$.

$$\text{Then } b + c + d + \dots + m = \bar{b} \cdot k + \bar{c} \cdot k + \dots + \bar{m} \cdot k = (\bar{b} + \bar{c} + \dots + \bar{m}) \cdot k - \text{the last product is}$$

divisible by k , then the initial sum is also divisible by k .

Proof of the uniqueness. Let's assume that some natural number a has two representations:

$$a = \partial_n 10^n + \partial_{n-1} 10^{n-1} + \dots + \partial_1 10 + \partial_0 \text{ and } a = \bar{\partial}_m 10^m + \bar{\partial}_{m-1} 10^{m-1} + \dots + \bar{\partial}_1 10 + \bar{\partial}_0, \text{ then}$$

$$\partial_n 10^n + \partial_{n-1} 10^{n-1} + \dots + \partial_1 10 + \partial_0 = \bar{\partial}_m 10^m + \bar{\partial}_{m-1} 10^{m-1} + \dots + \bar{\partial}_1 10 + \bar{\partial}_0.$$

Let's show that $\partial_0 = \bar{\partial}_0$. Let $\partial_0 \neq \bar{\partial}_0$, then

$$(\partial_n 10^n + \partial_{n-1} 10^{n-1} + \dots + \partial_1 10) - (\bar{\partial}_m 10^m + \bar{\partial}_{m-1} 10^{m-1} + \dots + \bar{\partial}_1 10) = \bar{\partial}_0 - \partial_0 \text{ the left part here is}$$

divisible by 10 (according to the **lemma3**), the right part $-9 \leq \bar{\partial}_0 - \partial_0 \leq 9$ (because $0 \leq \bar{\partial}_0 \leq 9$ and

$0 \leq \partial_0 \leq 9$). Among the numbers $\{-9, -8, \dots, -1, 0, 1, 2, \dots, 8, 9\}$ only 0 is divisible by 10 (because

$0 = 0 \cdot 10$). Then $\bar{\partial}_0 - \partial_0 = 0 \Rightarrow \bar{\partial}_0 = \partial_0$. Let's return to the initial equality

$\partial_n 10^n + \partial_{n-1} 10^{n-1} + \dots + \partial_1 10 + \partial_0 = \bar{\partial}_m 10^m + \bar{\partial}_{m-1} 10^{m-1} + \dots + \bar{\partial}_1 10 + \bar{\partial}_0$ here we can subtract $\bar{\partial}_0 = \partial_0$ from both sides, then $\partial_n 10^n + \partial_{n-1} 10^{n-1} + \dots + \partial_1 10 = \bar{\partial}_m 10^m + \bar{\partial}_{m-1} 10^{m-1} + \dots + \bar{\partial}_1 10$, let's use the distributive law for each part: $10 \cdot (\partial_n 10^{n-1} + \partial_{n-1} 10^{n-2} + \dots + \partial_1) = 10 \cdot (\bar{\partial}_m 10^{m-1} + \bar{\partial}_{m-1} 10^{m-2} + \dots + \bar{\partial}_1)$ here we have the equality like $10 \cdot b = 10 \cdot c$, if $b > c$, then $10 \cdot b > 10 \cdot c$ and if $b < c$, then $10 \cdot b < 10 \cdot c$, then $b = c$. So $\partial_n 10^{n-1} + \partial_{n-1} 10^{n-2} + \dots + \partial_1 = \bar{\partial}_m 10^{m-1} + \bar{\partial}_{m-1} 10^{m-2} + \dots + \bar{\partial}_1$ and we have the situation which is exactly similar to the initial one, then $\partial_1 = \bar{\partial}_1$ and etc. Then we will get $\partial_2 = \bar{\partial}_2, \partial_3 = \bar{\partial}_3 \dots$ after each step we subtract equal numbers $\partial_2 = \bar{\partial}_2, \partial_3 = \bar{\partial}_3 \dots$ from both sides.

Obviously, this process will finish soon. Let's assume that we came to the situation when there are no numbers left on the left or on the right part of the equality. Without loss of generality, let there are no numbers on the left part, then $0 = \bar{\partial}_m 10^m + \bar{\partial}_{m-1} 10^{m-1} + \dots + \bar{\partial}_k$. As $1 \leq \bar{\partial}_m \leq 9$ and $0 \leq \bar{\partial}_{m-1} \leq 9 \dots 0 \leq \bar{\partial}_k \leq 9$, the right part is a positive natural number, but there is a zero on the left side, and the equality is not true. Then the only possible case is when there are no numbers left on the both sides of the equality, and it looks like $0 = 0$.

Then $\bar{\partial}_0 = \partial_0, \partial_1 = \bar{\partial}_1, \partial_2 = \bar{\partial}_2 \dots \partial_n = \bar{\partial}_m \Rightarrow m = n$ and the representations:

$a = \partial_n 10^n + \partial_{n-1} 10^{n-1} + \dots + \partial_1 10 + \partial_0$ and $a = \bar{\partial}_m 10^m + \bar{\partial}_{m-1} 10^{m-1} + \dots + \bar{\partial}_1 10 + \bar{\partial}_0$ are exactly the same. The uniqueness is proved. And the **main theorem** is proved.

Def. Let and $a \in \mathbb{N} \parallel a > 10$ and $a = \partial_n 10^n + \partial_{n-1} 10^{n-1} + \dots + \partial_1 10 + \partial_0$ [E]- the representation from the main theorem. The sum on the right side can be denoted as:

$\partial_n \partial_{n-1} \dots \partial_1 \partial_0 \equiv / \text{by def} / \equiv \partial_n 10^n + \partial_{n-1} 10^{n-1} + \dots + \partial_1 10 + \partial_0$ and this symbol is called a decimal notation of a . As $\partial_n \partial_{n-1} \dots \partial_1 \partial_0$ defines the sum which is equal to a , we can write

$$a = \partial_n \partial_{n-1} \dots \partial_1 \partial_0.$$

Sometimes, in order to avoid ambiguity, we can draw the line above the symbol $\overline{\partial_n \partial_{n-1} \dots \partial_1 \partial_0}$, because $\partial_n \partial_{n-1} \dots \partial_1 \partial_0$ can be misunderstood as a product of numbers $\partial_n, \partial_{n-1} \dots \partial_1, \partial_0$.

Def [extension of the previous one]. Let $a \in \mathbb{Z}$ is an integer number. If $a \in \mathbb{N}$, then it's decimal notation is the symbol $\partial_n \partial_{n-1} \dots \partial_1 \partial_0$ (from above). If $a = 0$, then 0 is the decimal notation of a . If a is a negative number, then $a = -\Delta$ where $\Delta \in \mathbb{N}$, then the decimal notation of Δ with the minus sign in front of it is the decimal notation of a .

$$a = -\Delta \parallel \Delta \in \mathbb{N}, \Delta = \partial_n \partial_{n-1} \dots \partial_1 \partial_0 \Rightarrow a \equiv // \text{by def} // \equiv -\partial_n \partial_{n-1} \dots \partial_1 \partial_0$$

Conclusion: Any integer number $a \in \mathbb{Z}$ can be uniquely represented as a combination of symbols $0, 1, 2, 3 \dots 9$ with or without minus sign "-" in front of this combination. Such representation is called a decimal notation of a .

Divisibility

Exercise. [A] $a, b, c \in \mathbb{Z}$. If $a = b \cdot c$, then a is divisible by both b and c . **[B]** If a is divisible by b and b is divisible by c , then a is divisible by c . **[C]** Let $a = b + c$, if some two of these numbers are divisible by k , then the third (the other number) is also divisible by k .

Def. If natural numbers a and b do not have any common divisors except 1, then we write $(a, b) = 1$. And in this case we say that a and b are coprime numbers. In general, if some number d is the greatest common divisor of natural numbers a and b , then we write $(a, b) = d$.

Theorem 7. The given definition is correct, for any natural numbers $a, b \in \mathbb{N}$ there always exist a unique greatest common divisor d , moreover, there exist the pair of integer numbers λ, μ such that $\lambda \cdot a + \mu \cdot b = d$.

Proof. Let's consider the set $X \equiv \{m \cdot a + n \cdot b \mid m, n \in \mathbb{Z}\}$ of integer numbers, here a and b are fixed and m, n can be any integers. The set X is closed (as a subset of \mathbb{Z}) under addition/subtraction and multiplication by any $k \in \mathbb{Z}$. Also $a \in X$ ($m = 1, n = 0$) and $b \in X$ ($m = 0, n = 1$). As a, b are both positive, there exist a nonempty subset $N_X \subset X$ of natural numbers. There exist the least number $\bar{d} \in N_X$, this number is obviously the least positive number in X . Let's show that any element $x \in X$ is divisible by \bar{d} . We fix any $x \in X$.

According to the **2-nd part of the theorem 1 [division with a remainder]**, there exist the unique pair of integer numbers $k, r \mid 0 \leq r < \bar{d}$ such that $x = k \cdot \bar{d} + r$, then $r = x - k \cdot \bar{d}$.

Notice that $x, \bar{d} \in X \Rightarrow x - k \cdot \bar{d} \in X$. Then we have $r \in X$ and $0 \leq r < \bar{d}$. If $r > 0$ (positive), then we have a contradiction (because $r \in X$ and $r < \bar{d}$, but \bar{d} is the least positive number of X). Therefore $r = 0$ and $x = k \cdot \bar{d}$, so x is divisible by \bar{d} .

Notice that x is an arbitrary number from X .

Let's take $a, b \in X$, then $a = m \cdot \bar{d}$ and $b = n \cdot \bar{d}$ and also $\bar{d} \in X$, so there exist some (concrete) pair of integer numbers λ, μ such that $\lambda \cdot a + \mu \cdot b = \bar{d}$. From $a = m \cdot \bar{d}$ and $b = n \cdot \bar{d}$ follows that \bar{d} is a divisor of a and b , from the equality $\lambda \cdot a + \mu \cdot b = \bar{d}$ follows that there is no any other common divisor of a, b which is greater than \bar{d} . Really, if a and b are both divisible by some number $\tilde{d} > \bar{d}$, then the left part of $\lambda \cdot a + \mu \cdot b = \bar{d}$ is also divisible by \tilde{d} , then \bar{d} is divisible by \tilde{d} which is impossible (because $\tilde{d} > \bar{d}$). So, \bar{d} is not just a common divisor of numbers a, b , but it is also the greatest common divisor of these numbers $\bar{d} \equiv d$. And we also got the representation we need $\lambda \cdot a + \mu \cdot b = d$.

Consequence. $(a, b) = 1 \Leftrightarrow \lambda \cdot a + \mu \cdot b = 1$ for some integers $\lambda, \mu \in \mathbb{Z}$.

Def. A natural number $p \neq 1$ is called a **prime number** (or just a **prime**) if p is divisible only by 1 and p . Obviously: p is not a prime number $\Leftrightarrow p$ has some divisor b such that $1 < b < p$. The number 2 is the least prime number and the only prime number which is divisible by 2.

Assertion6. For any natural number $a > 1$ there exist at least one prime divisor p .

Proof. If a is a prime, then it is its own prime divisor, because $a = a \cdot 1$. Let a is not a prime, then it has some divisor $b \parallel 1 < b < a$. Then the set $X = \{all\ b \in \mathbb{N} \parallel a : b, b \neq 1, b \neq a\}$ of all divisors of a , which aren't equal to 1 or a , is not empty, therefore it contains the least number $m_{\min} \in X$. The number m_{\min} must be a prime number. Really, if m_{\min} is not a prime, then it has some divisor $d \parallel 1 < d < m_{\min}$, then d is also a divisor of a (**exercise [B]** above), then $d \in X$ and $d < m_{\min}$ and we have a contradiction. So m_{\min} is a prime divisor of a .

Exercise. The set P of all prime numbers is an infinite set.

Assertion7. Any natural number $a > 1$ can be represented as a product of several prime numbers.

Proof. Let's fix an arbitrary $a \in \mathbb{N}$. According to the **assertion6**, a has some prime divisor p , then $a = p \cdot \bar{a}$. If $\bar{a} = 1$, then $a = p$ is the representation we need. If $\bar{a} > 1$, then, according to the **assertion6**, \bar{a} has some prime divisor \bar{p} , then $\bar{a} = \bar{p} \cdot \bar{\bar{a}}$ and $a = p \cdot \bar{p} \cdot \bar{\bar{a}}$. If $\bar{\bar{a}} = 1$, then $a = p \cdot \bar{p}$ is the representation we need, if not, then we make the similar step as above.

We must show that this process must end at some moment.

Auxiliary. For any natural number a there exist $k \in \mathbb{N}$ such that $a < 2^k$. (It's very easy to prove by induction). Let's find and fix any $k \in \mathbb{N}$ such that $a < 2^k$. Then in the process, which is described above, there can't be more than k prime numbers on the right side of $a = p \cdot \bar{p} \cdot \bar{\bar{p}} \cdot \dots$.

Really, 2 is the least prime number and if there is more than k prime numbers on the right side, then the product on the right side is greater than 2^k , it means that $a > 2^k$, which contradicts to $a < 2^k$. So, the process, which is described above, must end for sure in $n < k$ steps.

We can also prove that for any $a > 1$ its representation as a product of primes is unique up to the order of prime numbers.

Let we have two representations: $a = p_1 \cdot p_2 \cdot \dots \cdot p_n$ and $a = \bar{p}_1 \cdot \bar{p}_2 \cdot \dots \cdot \bar{p}_m$.

Notice! When we have some representation, we do not multiply equal prime numbers, for example, $a = 2 \cdot 2 \cdot 2 \cdot 3$ is an appropriate representation, but we can't write it as $a = 2^3 \cdot 3$, because 2^3 is not a prime number.

We need to prove the auxiliary assertion.

Auxiliary. The product $b_1 \cdot b_2 \cdot \dots \cdot b_k$ is divisible by a prime number p , then at least one of the numbers b_1, b_2, \dots, b_k is divisible by p .

Proof. Let $k = 1$, then b_1 is divisible by p and the assertion is true.

Let's make an untypical step and prove the assertion for $k = 2$ (we will need it later).

So $b_1 \cdot b_2$ is divisible by p . If b_1 is divisible by p , then the assertion is true, if not, then $(b_1, p) = 1$.

Really, as p is a prime, 1 and p are the only divisors of p , therefore 1 is the only common divisor of numbers b_1, p . As $(b_1, p) = 1$, then there exist the representation $\lambda \cdot b_1 + \mu \cdot p = 1$, let's multiply by b_2 both sides of the last equality, we will get $\lambda \cdot (b_1 \cdot b_2) + \mu \cdot p \cdot b_2 = b_2$. The left part of the last equality is obviously divisible by p , then the right part (which is b_2) is also divisible by p . Everything is proved in the case $k = 2$.

If the assertion is true for a number k , let's consider it for $k + 1$. So $b_1 \cdot b_2 \cdot \dots \cdot b_k \cdot b_{k+1}$ is divisible by p . Let's designate $P \equiv b_1 \cdot b_2 \cdot \dots \cdot b_k$. The product of two numbers $P \cdot b_{k+1}$ is divisible by p , then one of these numbers is divisible by p . If $b_{k+1} \vdots p$, then everything is proved.

If $P \vdots p$, then the product $b_1 \cdot b_2 \cdot \dots \cdot b_k$ is divisible by p and (according to our assumption) one of the numbers b_1, b_2, \dots, b_k is divisible by p . The auxiliary assertion is proved.

Let $a = p_1 \cdot p_2 \cdot \dots \cdot p_n$ and $a = \bar{p}_1 \cdot \bar{p}_2 \cdot \dots \cdot \bar{p}_m$, then $p_1 \cdot p_2 \cdot \dots \cdot p_n = \bar{p}_1 \cdot \bar{p}_2 \cdot \dots \cdot \bar{p}_m$.

Let's list all the numbers from the left part and form the set $A = \{p_1, p_2, \dots, p_n\}$, and we also list all the numbers from the right part and form the set $B = \{\bar{p}_1, \bar{p}_2, \dots, \bar{p}_m\}$.

Let's take any prime number p_j from the left part, the product $p_1 \cdot p_2 \cdot \dots \cdot p_n$ is divisible by p_j , then the product $\bar{p}_1 \cdot \bar{p}_2 \cdot \dots \cdot \bar{p}_m$ must be also divisible by p_j . According to our auxiliary assertion, one of the numbers $\bar{p}_1, \bar{p}_2, \dots, \bar{p}_m$ is divisible p_j , so some \bar{p}_i is divisible by p_j .

If some prime number \bar{p}_i is divisible by a prime number p_j , then obviously $\bar{p}_i = p_j$.

We have shown: $\forall p_j \in A \Rightarrow p_j \in B$, therefore $A \subset B$. In the exactly similar way we can prove that $\forall \bar{p}_j \in B \Rightarrow \bar{p}_j \in A$, therefore $B \subset A$. Then $A = B$ and the representations of a are exactly the same (of course, up to the order of prime factors).

Def. G is any **commutative** additive group. We have already defined $na \parallel n \in \mathbb{N}$.

Now we also define: $0 \cdot a \equiv 0 \parallel \forall a \in G$. And for any negative number $(-n) \in \mathbb{Z} \parallel n \in \mathbb{N}$ we define: $-na \equiv -(na) \parallel \forall a \in G$.

Then all the previous basic properties are still true. For any elements $a, b \in G$ and for any $m, n \in \mathbb{Z}$

[A] $ma + na = (m + n)a$ [B] $m(a + b) = ma + mb$ [C] $mna = n(ma) = m(na)$

[D] $-(ma) = m(-a)$. The proof of each property must be done by considering all the possible variants: one of m, n is a zero number, both are natural, both negative, one is positive and the other one is negative. The proof is very simple, but a bit voluminous.

Def (similarly). G is a **commutative** multiplicative group. We have already defined $a^n \parallel n \in \mathbb{N}$.

Now we also define: $a^0 \equiv e$. For any negative number $(-n) \in \mathbb{Z} \parallel n \in \mathbb{N}$ we define $a^{-n} \equiv (a^n)^{-1}$.

For any elements $a, b \in G$ and for any $m, n \in \mathbb{Z}$ the next is true:

[A] $a^m \cdot a^n = a^{m+n}$ [B] $(a \cdot b)^m = a^m \cdot b^m$ [C] $a^{mn} = (a^m)^n = (a^n)^m$ [D] $(a^m)^{-1} = (a^{-1})^m$.



5

*Rational
numbers*

Rational numbers

Def. Q is the field that contains the ring Z of integer numbers. Any element $q \in Q$ can be represented as a ratio of some integers $q = \frac{a}{b}$. The addition and multiplication on Q are extensions of the addition and multiplication on Z , i.e., for any $a, b \in Z \subset Q$:

$a + b$ (addition by the rules of Q) = $a + b$ (addition by the rules of Z),
 $a \cdot b$ (multiplication by the rules of Q) = $a \cdot b$ (multiplication by the rules of Z).

The field Q is called a field of rational numbers and elements of Q are called rational numbers.

Let's build Q . We fix any set Z of integer numbers. Let's consider the set Ω of all pairs $\{(a, b)\}$ where $a \in Z, b \in Z \parallel b \neq 0$ are any integer numbers. We define addition and multiplication on Ω .

Def. $(a, b) \oplus (c, d) \equiv (a \cdot d + b \cdot c, b \cdot d)$ and $(a, b) \bullet (c, d) \equiv (a \cdot c, b \cdot d)$.

How to remember it? Imagine that any pair (a, b) denotes the ratio $\frac{a}{b}$ of elements a, b in some field.

Then $(a, b) \oplus (c, d) \leftrightarrow \frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d} \leftrightarrow (a \cdot d + b \cdot c, b \cdot d)$ and

$(a, b) \bullet (c, d) \leftrightarrow \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d} \leftrightarrow (a \cdot c, b \cdot d)$.

Moreover, we say that pairs (a, b) and (c, d) are equivalent $(a, b) \approx (c, d)$ if $a \cdot d = b \cdot c$.

It's very easy to see that \approx is really an equivalence relation, because it is reflexive, symmetric, transitive.

Assertion1. The addition " \oplus " and multiplication " \bullet " of pairs are both commutative and associative on Ω . And instead of distributivity we have the equivalence:
 $((a, b) \oplus (c, d)) \bullet (e, m) \approx ((a, b) \bullet (e, m)) \oplus ((c, d) \bullet (e, m))$ and
 $(e, m) \bullet ((a, b) \oplus (c, d)) \approx ((e, m) \bullet (a, b)) \oplus ((e, m) \bullet (c, d))$.

Proof. As the multiplication of integer numbers is associative and commutative, the multiplication of pairs is also commutative and associative. Next:

$(a, b) \oplus (c, d) \equiv (a \cdot d + b \cdot c, b \cdot d)$ and $(c, d) \oplus (a, b) \equiv (c \cdot b + d \cdot a, d \cdot b)$, then

$(a, b) \oplus (c, d) = (c, d) \oplus (a, b)$ (the addition of pairs is commutative).

And $((a, b) \oplus (c, d)) \oplus (e, m) \equiv (a \cdot d + b \cdot c, b \cdot d) \oplus (e, m) = ((a \cdot d + b \cdot c) \cdot m + b \cdot d \cdot e, b \cdot d \cdot m)$ and
 $(a, b) \oplus ((c, d) \oplus (e, m)) \equiv (a, b) \oplus (c \cdot m + d \cdot e, d \cdot m) = (a \cdot d \cdot m + b \cdot (c \cdot m + d \cdot e), b \cdot d \cdot m)$.

It's easy to compare the results and see that the addition of pairs \oplus is associative.

Let's finally consider $((a, b) \oplus (c, d)) \bullet (e, m) = (a \cdot d + b \cdot c, b \cdot d) \bullet (e, m) = ((a \cdot d + b \cdot c) \cdot e, b \cdot d \cdot m)$ and also the sum

$$\begin{aligned} ((a,b) \bullet (e,m)) \oplus ((c,d) \bullet (e,m)) &= (a \cdot e, b \cdot m) \oplus (c \cdot e, d \cdot m) = (a \cdot e \cdot d \cdot m + b \cdot m \cdot c \cdot e, b \cdot m \cdot d \cdot m) = \\ &= (m \cdot (a \cdot e \cdot d + b \cdot c \cdot e), m \cdot (b \cdot d \cdot m)) \text{ -this pair is obviously equivalent to } ((a \cdot d + b \cdot c) \cdot e, b \cdot d \cdot m). \end{aligned}$$

So, we have showed that $((a,b) \oplus (c,d)) \bullet (e,m) \approx (a,b) \bullet (e,m) \oplus (c,d) \bullet (e,m)$ [P].

The other distributivity-equivalence follows from [P] and commutativity of the pair multiplication \bullet . Everything is proved.

The equivalence relation of pairs divides Ω into the classes $A, B, C, D, E \dots$ of equivalent pairs.

The set of all classes we denote like \mathcal{Q}_{aux} . Let's define addition and multiplication on \mathcal{Q}_{aux} in order to turn \mathcal{Q}_{aux} into a field.

Def. Let A, B are any classes from \mathcal{Q}_{aux} . And $(a,b) \in A, (c,d) \in B$ are any pairs from these classes. The sum $A \oplus B$ is the class which contains the sum of pairs (a,b) and (c,d) , i.e., the pair $(a \cdot d + b \cdot c, b \cdot d) = (a,b) \oplus (c,d)$. The product $A \bullet B$ is the class which contains the product of pairs (a,b) and (c,d) , i.e., the pair $(a \cdot c, b \cdot d) = (a,b) \bullet (c,d)$.

Exercise1. Show that the given definition is correct. For any classes $A, B \in \mathcal{Q}_{aux}$, a sum $A \oplus B$ and a product $A \bullet B$ are uniquely defined.

Exercise2. The set $(\mathcal{Q}_{aux}, \oplus, \bullet)$ (of all classes) is a field.

Solution. The addition of pairs is associative and commutative, therefore the addition of classes is also associative and commutative on \mathcal{Q}_{aux} . The “zero” class O is the class which contains the pair $(0,1)$. The zero class obviously consists of the pairs $(0,b) \parallel b \in \mathbb{Z}, b \neq 0$. For any class A with a pair (a,b) , an opposite class $-A$ is the class with the pair $(-a,b)$. So \mathcal{Q}_{aux} is a commutative group with respect to addition. The multiplication of classes is associative, because the multiplication of pairs is associative. And finally, there is a distributive law for classes of \mathcal{Q}_{aux} , it follows from the “distributive equivalence” for pairs, that is proved in the [assertion1](#). Then $(\mathcal{Q}_{aux}, \oplus, \bullet)$ is a ring.

We have to show now that all nonzero classes of \mathcal{Q}_{aux} form a commutative group with respect to \bullet .

[step1] $\mathcal{Q}_{aux} \setminus O$ is closed under multiplication (a very important requirement). Really, let's take any $A, B \in \mathcal{Q}_{aux} \setminus O$, both these classes are non-zero classes, then for any $(a,b) \in A \Rightarrow a \neq 0$ and for any $(c,d) \in B \Rightarrow c \neq 0$. The class $A \bullet B$ contains the pair $(a \cdot c, b \cdot d)$ and $a \cdot c \neq 0$ (because integer numbers a, b are not zeroes), then $A \bullet B$ is not a zero class, so $A \bullet B \in \mathcal{Q}_{aux} \setminus O$. As the multiplication of pairs is commutative, the multiplication of classes \bullet is also commutative on all \mathcal{Q}_{aux} , as $\mathcal{Q}_{aux} \setminus O$ is closed under multiplication, the multiplication of classes \bullet is commutative on $\mathcal{Q}_{aux} \setminus O$. And similarly, the multiplication of classes is associative on $\mathcal{Q}_{aux} \setminus O$.

[step2] The class “one” I is the class which contains the pair $(1,1)$ and obviously $I \in \mathcal{Q}_{aux} \setminus O$. Also, for any nonzero class $A \in \mathcal{Q}_{aux} \setminus O$ with a pair (a,b) (here $a \neq 0$ because $A \neq O$) an inverse class A^{-1} is the class with the pair (b,a) and obviously $A^{-1} \in \mathcal{Q}_{aux} \setminus O$ (because $b \neq 0$).

Then $Q_{aux} \setminus O$ is a commutative multiplicative group, and $(Q_{aux}, \oplus, \bullet)$ is a field.

Def: a class $A \in Q_{aux}$ with a pair (a, b) is called positive if $a \cdot b > 0$.

Exercise3. Show that:

- [1] The given definition is correct. If $a \cdot b > 0$ for some pair $(a, b) \in A$, then $c \cdot d > 0$ for any pair $(c, d) \in A$.
- [2] For any class $A \in Q_{aux}$ only one of the next cases is true:
A is positive, **or** $-A$ is positive, **or** $A = 0$.
- [3] If classes A, B are positive, then both $A \oplus B$ and $A \bullet B$ are positive.

From the **exercise3** immediately follows that Q_{aux} is an ordered field (the order ">" on Q_{aux} appears "automatically" by the rule: $A > B$ in Q_{aux} if $A - B$ is a positive class).

Exercise4. For any integer number $k \in \mathbb{Z}$ there exist the unique class $A \in Q_{aux}$, such that for any $(a, b) \in A$ we have $a = k \cdot b$ (let's fix any $k \in \mathbb{Z}$ and take the class A with the pair $(k, 1)$, for any other pair $(a, b) \in A$ there must be $(a, b) \approx (k, 1) \Rightarrow a = k \cdot b$).

Let's build the set Q . Any class $A \in Q_{aux}$ such that $a = k \cdot b \ \forall (a, b) \in A$ (for some integer number $k \in \mathbb{Z}$) we call an integer class. Let $Z_{classes}$ is the set of all integer classes of Q_{aux} . Every integer class $A = \{(k \cdot b, b) \mid k \in \mathbb{Z} \text{ (is fixed), } b \in \mathbb{Z}, b \neq 0\}$ we replace by $k \in \mathbb{Z}$, we will get the set $Q = \mathbb{Z} \cup (\text{classes of pairs})$.

The set Q is called a set of **rational numbers**, it consists of integer numbers and classes of equivalent pairs. Let's define addition and multiplication on Q in order to turn Q into a field.

$$\begin{array}{ccc} & Z_{classes} & (\text{classes of pairs}) \\ & \downarrow & \downarrow \\ \text{We define the mapping } f : Q_{aux} \rightarrow Q & \Leftrightarrow & \end{array}$$

For any integer class $A = \{(k \cdot b, b) \mid k \in \mathbb{Z} \text{ (is fixed), } b \in \mathbb{Z}, b \neq 0\}$ we define $f(A) \equiv k$ and $f(B) \equiv B$ for any other class $B \in Q_{aux}$. Then f is obviously one-to-one mapping $Q_{aux} \rightarrow Q$.

Any element $a \in Q$ can be uniquely represented as an image of some class $a = f(A) \mid A \in Q_{aux}$.

Then we define $\forall a, b \in Q \Rightarrow$

$$\begin{aligned} a + b &= f(A) + f(B) \equiv / \text{by definition} / \equiv f(A \oplus B) \in Q \\ a \cdot b &= f(A) \cdot f(B) \equiv / \text{by definition} / \equiv f(A \bullet B) \in Q \end{aligned}$$

From the **theorem4** ("Groups, Rings, Fields") immediately follows that $(Q, +, \cdot)$ is a field.

According to the **theorem5 (Transfer of order)**, Q is an ordered field. The field $(Q, +, \cdot)$ is called a field of rational numbers. Let's explore the properties of this field.

Property1. The addition and multiplication on Q are extensions of the addition and multiplication on Z , i.e., for any $a, b \in Z \subset Q$ we have:

$$a + b \text{ (addition by the rules of } Q) = a + b \text{ (addition by the rules of } Z),$$

$$a \cdot b \text{ (multiplication by the rules of } Q) = a \cdot b \text{ (multiplication by the rules of } Z).$$

And similarly, the order relation ">" on Q is an extension of the order relation on Z :

$$a > b \text{ (by the rules of } Q) \Leftrightarrow a > b \text{ (by the rules of } Z).$$

Proof. Let's denote for a while $(\tilde{+}, \tilde{\cdot})$ - the addition and multiplication on the field Q and $(+, \cdot)$ - the addition and multiplication on the ring Z .

Let's fix arbitrary integer numbers $a, b \in Z \subset Q$. In order to find the sum $a \tilde{+} b$ (in Q) we need to find the classes A, B (from Q_{aux}) such that $f(A) = a$, $f(B) = b$ then, by definition,

$a \tilde{+} b = f(A) \tilde{+} f(B) \equiv f(A \oplus B)$. Obviously, A is the class with the pair $(a, 1)$ and B is the class with the pair $(b, 1)$. Then $A \oplus B$ contains the pair $(a, 1) \oplus (b, 1) = (a + b, 1)$, therefore $A \oplus B$ is an integer class and $f(A \oplus B) = a + b$. So $a \tilde{+} b = a + b$ for any $a, b \in Z \subset Q$.

Next, $a \tilde{\cdot} b = f(A) \tilde{\cdot} f(B) \equiv f(A \bullet B)$ and $A \bullet B$ is the class which contains the pair $(a, 1) \bullet (b, 1) = (a \cdot b, 1)$, then $A \bullet B$ is an integer class and $f(A \bullet B) = a \cdot b$,

so $a \tilde{\cdot} b = a \cdot b$ for any $a, b \in Z \subset Q$. And finally, let $a > b$ (in Q) $\Leftrightarrow f(A) > f(B)$ (in Q) \Leftrightarrow

$\Leftrightarrow // f \text{ conserves the order } ">" // \Leftrightarrow A > B$ (in Q_{aux}), then the class $(A - B) = A \oplus (-B)$ is positive in Q_{aux} . Here $(a, 1) \in A$, $(-b, 1) \in (-B) \Rightarrow$ the class $A \oplus (-B)$ contains the pair $(a - b, 1)$, as this class is positive, there must be $(a - b) \cdot 1 > 0 \Rightarrow a - b > 0 \Rightarrow a > b$ (in Z).

Conversely, let $a > b$ (in Z). Let's consider the class A such that $(a, 1) \in A$ and the class B such that $(b, 1) \in B$. The class $A - B$, which contains the pair $(a - b, 1)$, is positive, then

$$A > B \text{ (in } Q_{aux}) \Rightarrow f(A) > f(B) \text{ (in } Q) \Leftrightarrow a > b \text{ (in } Q).$$

Conclusion. The order relation/ addition/multiplication on Q are all extensions of the order relation/ addition/multiplication on Z . Then it's appropriate to use exactly the same signs ($< + \cdot$) (as we used on Z) to denote these operations on Q . Remember that ($< + \cdot$) on Z are extensions of ($< + \cdot$) on N . Then ($< + \cdot$) on Q are also extensions of ($< + \cdot$) on N . All natural numbers are positive (greater than zero) in Q , because they are positive in Z .

As Q is a field, division ":" is defined on Q (the only restriction, we can't divide by zero).

If $a, m, n \in Q$ and $a = \frac{m}{n}$, then we say " a is a ratio of numbers m and n ".

Property2. Every element of $a \in Q$ can be represented as a ratio of some integer numbers

$$a = \frac{m}{n} \parallel m, n \in Z \text{ (and such representation is not unique).}$$

Proof. Let's fix an arbitrary $a \in Q$, it has the unique representation $a = f(A) \parallel A \in Q_{aux}$.

Let's take any pair $(m, n) \in A$. Obviously $(n, 1) \bullet (m, n) \approx (m, 1)$, then $B \bullet A = C$, where B is the integer class with the pair $(n, 1)$ and C is the integer class with the pair $(m, 1)$. Then

$$f(B \bullet A) = f(C) \Rightarrow f(B) \cdot f(A) = f(C) \Rightarrow n \cdot a = m \text{ (in } Q) \Rightarrow a = \frac{m}{n}.$$

This representation is not unique, really if $a = \frac{m}{n} \parallel m, n \in Z$, then (according to the basic properties of any field)

$$a = \frac{q \cdot m}{q \cdot n} \text{ for any } q \in Q \parallel q \neq 0 \text{ and in particular } a = \frac{k \cdot m}{k \cdot n} \text{ for any } k \in Z \subset Q \parallel k \neq 0.$$

Property3. Q is a minimal field that contains Z . It means that:

any other field F , which contains Z , contains Q as a subfield. (as earlier, when we say that some field F contains Z , we mean not only that F contains **the set** Z , but also that addition and multiplication on F are extensions of the addition and multiplication on Z).

Proof. Let some field F contains Z . Then F must contain all the ratios of elements from Z , i.e., all the elements $\tilde{Q} = \left\{ \frac{m}{n} \parallel m, n \in Z, n \neq 0 \right\}$. So F contains the set \tilde{Q} . Obviously $Z \subset \tilde{Q}$,

$$\text{because } \forall a \in Z: a = \frac{a}{1} \in \tilde{Q}.$$

The set \tilde{Q} consists of exactly the same elements as a field of rational numbers Q ([property 2](#)).

Let's show that **the set** \tilde{Q} is a subfield of F . According to the basic properties of any field (which we mentioned earlier), we have:

$$\frac{m}{n} \pm \frac{k}{p} = \frac{m \cdot p \pm n \cdot k}{n \cdot p}, \quad \frac{m}{n} \cdot \frac{k}{p} = \frac{m \cdot k}{n \cdot p}, \quad \frac{m}{n} : \frac{k}{p} = \frac{m \cdot p}{n \cdot k}.$$

So, the sum/difference/product/ratio of any elements of \tilde{Q} belong to \tilde{Q} . Therefore \tilde{Q} is a subfield of F (subfield criterion).

Then \tilde{Q} is an independent field inside F . And finally, as addition/multiplication on F are extensions of the addition/multiplication on Z , then addition/multiplication on $\tilde{Q} \supset Z$ are extensions of the addition/multiplication on Z .

Then, by definition, \tilde{Q} is a field of rational numbers and a subfield of F .

Uniqueness. We have built the field of rational numbers Q , based on some set Z of integer numbers which we have fixed at the very beginning. There exist different sets of integer numbers (but all of them are isomorphic as rings). Let's prove:

The uniqueness theorem. Any fields Q_A and Q_B of rational numbers are isomorphic.

Moreover, the isomorphism $f : Q_A \rightarrow Q_B$ is unique, this isomorphism is an extension of the unique isomorphism $f : Z_A \rightarrow Z_B$.

Proof. Existence. Let's extend the unique isomorphism $f : Z_A \rightarrow Z_B$ up to $f : Q_A \rightarrow Q_B$.

We define: for any $a_A \in Q_A$ if $a_A = \frac{m_A}{n_A} \parallel m_A, n_A \in Z_A$, then $f(a_A) \equiv \frac{f(m_A)}{f(n_A)} \parallel f(m_A), f(n_A) \in Z_B$.

At first, we need to show that this definition is correct, for any element $a_A \in Q_A$ the element $f(a_A) \in Q_B$ is uniquely defined, it follows from [A] and [B]. **Secondly**, we need to show that the new isomorphism is really an extension of the old one, it follows from [C].

[A] In any representation $a_A = \frac{m_A}{n_A}$ the number $n_A \neq 0_A$, then in $f(a_A) \equiv \frac{f(m_A)}{f(n_A)}$, the number $f(n_A) \neq 0_B$ (because $f : Z_A \rightarrow Z_B$ is a ring isomorphism, and it transfers zero into zero $f(0_A) = 0_B$). From here follows that for any $a_A \in Q_A$ the element(s) $f(a_A) \in Q_B$ exists.

[B] If $a_A = \frac{m_A}{n_A}$ and $a_A = \frac{\tilde{m}_A}{\tilde{n}_A}$ are different representations of $a_A \in Q_A$, let's show that

$$f(a_A) = \frac{f(m_A)}{f(n_A)} = \frac{f(\tilde{m}_A)}{f(\tilde{n}_A)} \text{ (from here will follow that for any } a_A \in Q_A \text{ the element } f(a_A) \in Q_B \text{ is}$$

unique). So $\frac{m_A}{n_A} = \frac{\tilde{m}_A}{\tilde{n}_A} \Rightarrow m_A \cdot \tilde{n}_A = n_A \cdot \tilde{m}_A$ the last equality is an equality of integer numbers in

Z_A , and f is a ring isomorphism $f : Z_A \rightarrow Z_B$, then

$$f(m_A \cdot \tilde{n}_A) = f(n_A \cdot \tilde{m}_A) \Rightarrow f(m_A) \cdot f(\tilde{n}_A) = f(n_A) \cdot f(\tilde{m}_A) \text{ the last equality is an equality in } Q_B,$$

here $f(n_A) \neq 0_B$ and $f(\tilde{n}_A) \neq 0_B$ (because $n_A \neq 0_A$, $\tilde{n}_A \neq 0_A$), then $\frac{f(m_A)}{f(n_A)} = \frac{f(\tilde{m}_A)}{f(\tilde{n}_A)}$.

After [A] and [B] we can say that f is a mapping $Q_A \rightarrow Q_B$.

[C] The new mapping f coincides with the old mapping f on the set $Z_A \subset Q_A$. For the initial isomorphism we had $\forall m_A \in Z_A \Rightarrow m_A \xrightarrow{f} f(m_A) \in Z_B$, according to the new rules we need to

represent m_A as a ratio of any integers, and then we can find it's image. Let's take $m_A = \frac{m_A}{1_A}$,

$$\text{then according to the new rules, } m_A = \frac{m_A}{1_A} \xrightarrow{f} \frac{f(m_A)}{f(1_A)} = \frac{f(m_A)}{1_B} = f(m_A).$$

So, the new mapping coincides with the initial mapping on Z_A .

Let's show that $f : Q_A \rightarrow Q_B$ is one-to-one. By definition of f , we have

$$f\left(\frac{m_A}{n_A}\right) = \frac{f(m_A)}{f(n_A)} \parallel \forall m_A, n_A \in Z_A.$$

[Step1] f covers all Q_B . Let's fix any $a_B \in Q_B$, there exist the representation

$$a_B = \frac{m_B}{n_B} \parallel m_B, n_B \in Z_B. \text{ As } f : Z_A \rightarrow Z_B \text{ is one-to-one, then there exist unique}$$

$$m_A, n_A \in Z_A \parallel f(m_A) = m_B, f(n_A) = n_B, \text{ so } a_B = \frac{m_B}{n_B} = \frac{f(m_A)}{f(n_A)} = f\left(\frac{m_A}{n_A}\right) \text{ and } a_B \text{ is an image of}$$

the element $\frac{m_A}{n_A} \equiv a_A \in Q_A$.

[Step2] f doesn't glue together elements of Q_A . Let for some elements $a_A, b_A \in Q_A$ we have:

$a_A \neq b_A$, but $f(a_A) = f(b_A)$. Both elements a_A, b_A have representations

$$a_A = \frac{m_A}{n_A}, b_A = \frac{k_A}{p_A} \parallel m_A, n_A, k_A, p_A \in Z. \text{ Then } f(a_A) = \frac{f(m_A)}{f(n_A)} \text{ and } f(b_A) = \frac{f(k_A)}{f(p_A)}.$$

As $f(a_A) = f(b_A)$, then $\frac{f(m_A)}{f(n_A)} = \frac{f(k_A)}{f(p_A)} \Rightarrow f(m_A) \cdot f(p_A) = f(n_A) \cdot f(k_A)$ the last equality can

be rewritten like $f(m_A \cdot p_A) = f(n_A \cdot k_A)$ (because $f : Z_A \rightarrow Z_B$ is a ring isomorphism), as f is one-to-one, then $m_A \cdot p_A = n_A \cdot k_A$ -it is an equality in Z_A , in the same time it is an equality in Q_A ,

from which follows that $\frac{m_A}{n_A} = \frac{k_A}{p_A}$ (notice that $n_A \neq 0_A, p_A \neq 0_A$, because $f(n_A) \neq 0_B, f(p_A) \neq 0_B$)

and the last equality means that $a_A = b_A$, and we have a contradiction.

So $f : Q_A \rightarrow Q_B$ is one-to-one. Let's finally show that f is a field isomorphism:

$\forall a_A, b_A : f(a_A + b_A) = f(a_A) + f(b_A)$ and $f(a_A \cdot b_A) = f(a_A) \cdot f(b_A)$. Let's fix arbitrary

$a_A, b_A \in Q_A$, we fix any representations $a_A = \frac{m_A}{n_A}, b_A = \frac{k_A}{p_A}$. Then

$$\begin{aligned} f(a_A + b_A) &= f\left(\frac{m_A}{n_A} + \frac{k_A}{p_A}\right) = f\left(\frac{m_A \cdot p_A + n_A \cdot k_A}{n_A \cdot p_A}\right) = \frac{f(m_A \cdot p_A + n_A \cdot k_A)}{f(n_A \cdot p_A)} = \frac{f(m_A \cdot p_A) + f(n_A \cdot k_A)}{f(n_A \cdot p_A)} = \\ &= \frac{f(m_A) \cdot f(p_A) + f(n_A) \cdot f(k_A)}{f(n_A) \cdot f(p_A)} = \frac{f(m_A)}{f(n_A)} + \frac{f(k_A)}{f(p_A)} = f\left(\frac{m_A}{n_A}\right) + f\left(\frac{k_A}{p_A}\right) = f(a_A) + f(b_A). \end{aligned}$$

$$\begin{aligned} \text{And } f(a_A \cdot b_A) &= f\left(\frac{m_A}{n_A} \cdot \frac{k_A}{p_A}\right) = f\left(\frac{m_A \cdot k_A}{n_A \cdot p_A}\right) = \frac{f(m_A \cdot k_A)}{f(n_A \cdot p_A)} = \frac{f(m_A) \cdot f(k_A)}{f(n_A) \cdot f(p_A)} = \frac{f(m_A)}{f(n_A)} \cdot \frac{f(k_A)}{f(p_A)} = \\ &= f\left(\frac{m_A}{n_A}\right) \cdot f\left(\frac{k_A}{p_A}\right) = f(a_A) \cdot f(b_A). \end{aligned}$$

The existence of isomorphism $f : Q_A \rightarrow Q_B$ is proved.

Uniqueness. We have already built $f: Q_A \rightarrow Q_B$ which is an extension of $f: Z_A \rightarrow Z_B$.

Let $\varphi: Q_A \rightarrow Q_B$ is a field isomorphism, we will show that $\varphi \equiv f$ on Q_A .

As $\varphi: Q_A \rightarrow Q_B$ is a field isomorphism, then it transfers zero into zero and one into one: $\varphi(0_A) = 0_B$ and $\varphi(1_A) = 1_B$. Let's take $Z_A \subset Q_A$ and $Z_B \subset Q_B$. Let's show that φ is an isomorphism of the rings $Z_A \rightarrow Z_B$.

At first we need to show that all the values of φ on Z_A belong to Z_B .

We have: $Z_A = -N_A \cup 0_A \cup N_A$ and $Z_B = -N_B \cup 0_B \cup N_B$.

So $Z_A = -N_A \cup 0_A \cup N_A$. If $a_A \in N_A$, then a_A can be represented as a sum of ones,

$a_A = 1_A + 1_A + \dots + 1_A$, then

$$\varphi(a_A) = \varphi(1_A + 1_A + \dots + 1_A) = \varphi(1_A) + \varphi(1_A) + \dots + \varphi(1_A) = 1_B + 1_B + \dots + 1_B \equiv a_B \in N_B \subset Z_B.$$

If $a_A = 0_A$, then $\varphi(0_A) = 0_B \in Z_B$. If $a_A \in -N_A$, then $a_A = -\tilde{a}_A$ || $\tilde{a}_A \in N_A$, then

$a_A = -\tilde{a}_A = -(1_A + 1_A + \dots + 1_A)$, then

$$\begin{aligned} \varphi(a_A) &= \varphi(-\tilde{a}_A) = \varphi(-(1_A + 1_A + \dots + 1_A)) = -\varphi(1_A + 1_A + \dots + 1_A) = -(\varphi(1_A) + \varphi(1_A) + \dots + \varphi(1_A)) = \\ &= -(1_B + 1_B + \dots + 1_B) = -a_B \in -N_B \in Z_B. \end{aligned}$$

Only now we can write $\varphi: Z_A \rightarrow Z_B$ and say that φ is a mapping from Z_A to Z_B .

[Step1] Let's show that $\varphi: Z_A \rightarrow Z_B$ covers all the set Z_B . So $Z_B = -N_B \cup 0_B \cup N_B$.

Let $a_B \in Z_B$, there can be several variants. If $a_B \in N_B$, then a_B can be represented as a sum of ones, so $a_B = 1_B + 1_B + \dots + 1_B = \varphi(1_A) + \varphi(1_A) + \dots + \varphi(1_A) = \varphi(1_A + 1_A + \dots + 1_A) \equiv \varphi(a_A)$ || $a_A \in N_A$ and a_B is the image of $a_A \in Z_A$.

If $a_B = 0_B$, then $\varphi(0_A) = 0_B$ and 0_B is the image of $0_A \in Z_A$.

If $a_B \in -N_B$, then $a_B = -\tilde{a}_B = -(1_B + 1_B + \dots + 1_B) =$

$$= -(\varphi(1_A) + \varphi(1_A) + \dots + \varphi(1_A)) = -\varphi(1_A + 1_A + \dots + 1_A) = -\varphi(a_A) || a_A \in N_A = \varphi(-a_A) || -a_A \in -N_A$$

and a_B is the image of $-a_A \in Z_A$. So, any element $a_B \in Z_B$ is an image of some element from Z_A .

[Step2] φ doesn't glue together elements of Z_A , because φ doesn't glue together elements of Q_A (really, φ is an isomorphism $\varphi: Q_A \rightarrow Q_B$, then it is one-to-one mapping).

From the **[Step1]** and **[Step2]** follows that $\varphi: Z_A \rightarrow Z_B$ is one-to-one.

[Step3] For any $\forall a_A, b_A \in Z_A$ we have $\varphi(a_A + b_A) = \varphi(a_A) + \varphi(b_A)$ and $\varphi(a_A \cdot b_A) = \varphi(a_A) \cdot \varphi(b_A)$.

Really, these conditions are true for any $\forall a_A, b_A \in Q_A$, because $\varphi: Q_A \rightarrow Q_B$ is an isomorphism, and in particular these conditions are true for any $\forall a_A, b_A \in Z_A$.

From the **[Step3]** follows that φ is an isomorphism of the rings $Z_A \rightarrow Z_B$. And we have proved that there exist only one isomorphism $f: Z_A \rightarrow Z_B$, then $\varphi \equiv f$ on Z_A . Let's show $\varphi \equiv f$ on Q_A .

Let's fix an arbitrary $a_A \in Q_A$ and any it's representation as a ratio of integers $a_A = \frac{m_A}{n_A}$.

We know that $f(a_A) \equiv \frac{f(m_A)}{f(n_A)}$. Obviously $f(m_A) = \varphi(m_A)$ (because $m_A \in Z_A$) and similarly

$f(n_A) = \varphi(n_A)$ (because $n_A \in Z_A$), then $f(a_A) = \frac{f(m_A)}{f(n_A)} = \frac{\varphi(m_A)}{\varphi(n_A)}$. Let's show that $\varphi(a_A)$ is also

equal to $\frac{\varphi(m_A)}{\varphi(n_A)}$, then $\varphi(a_A) = f(a_A)$ for any $a_A \in Q_A$ and $\varphi \equiv f$ on Q_A .

So $a_A = \frac{m_A}{n_A} \Rightarrow a_A \cdot n_A = m_A$ the last equality is an equality in Q_A and $\varphi: Q_A \rightarrow Q_B$ is one-to-one

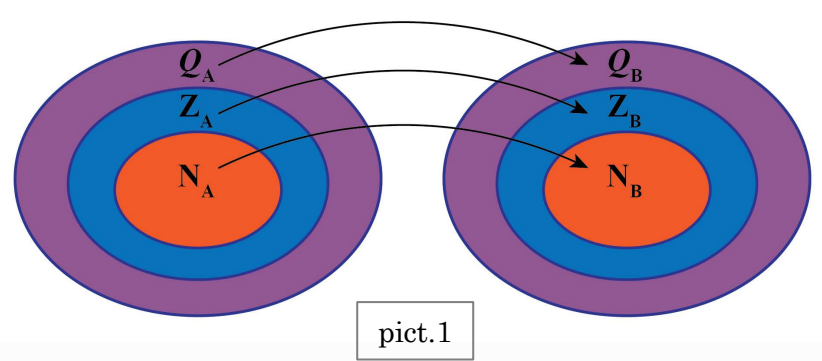
mapping, then $\varphi(a_A \cdot n_A) = \varphi(m_A)$, as φ is an isomorphism, then

$$\varphi(a_A \cdot n_A) = \varphi(m_A) \Rightarrow \varphi(a_A) \cdot \varphi(n_A) = \varphi(m_A).$$

Let's notice that $\varphi(n_A) \neq 0_B$ because $n_A \neq 0_A$, then from the last equality we have $\varphi(a_A) = \frac{\varphi(m_A)}{\varphi(n_A)}$.

Everything is proved.

Consequence. For any fields of integer numbers Q_A, Q_B there exist the unique isomorphism $f: Q_A \rightarrow Q_B$ which is an extension of the unique isomorphism $f: Z_A \rightarrow Z_B$ (where $Z_A \subset Q_A, Z_B \subset Q_B$) which, in it's turn, is an extension of the unique isomorphism $f: N_A \rightarrow N_B$ (where $N_A \subset Z_A \subset Q_A, N_B \subset Z_B \subset Q_B$) [pict1].



Property4. The Archimedes axiom is true in Q .

Proof. Let's fix any positive numbers $a, b \in Q$. We want to show that there exist $n \in N \subset Q$ such

that $n \cdot a > b$. The element $\frac{1}{a}$ is positive, then the last inequality is equivalent to $n > \frac{b}{a}$, where $\frac{b}{a}$

is a positive element of Q . Let's show that for any positive element $q \in Q$ there exist the natural $n \in N$ such that $n > q$ (and everything will be proved). We fix an arbitrary positive $q > 0$, then

$q = \frac{k}{p} \parallel k, p \in Z$. The fraction $\frac{k}{p}$ is positive, then $k \cdot p$ is positive, then $k \cdot p$ is a natural number.

Then $k \cdot p \geq 1$, let's multiply both sides of $k \cdot p \geq 1$ by $\frac{k}{p} > 0 \Rightarrow$

$$\frac{k}{p} \cdot k \cdot p > \frac{k}{p} \cdot 1 \Leftrightarrow k^2 > \frac{k}{p} \Leftrightarrow k^2 > q \parallel k^2 \in N, \text{ everything is proved.}$$

Property5. For any rational number $q \in \mathbb{Q}$ there exist the unique pair of integer numbers $k, k+1$ such that $k \leq q < k+1$.

Existence. Let's fix an arbitrary **positive** rational number q . Let's consider the pair $1, q$.

If $q < 1$, then we have $0 < q < 1$ and the pair of integers $k, k+1 \equiv 0, 1$ is appropriate.

If $q \geq 1$, then $1 \cdot 1 \leq q$ and the set of natural numbers $X \equiv \{m \mid m \cdot 1 \leq q\}$ is not empty.

According to the **Archimedes axiom**, there exist the natural number n such that $n \cdot 1 > q$.

The number n is greater than any number of the set X , therefore X has the greatest number M_{\max} . And for M_{\max} we obviously have $M_{\max} \cdot 1 \leq q < (M_{\max} + 1) \cdot 1 \Leftrightarrow M_{\max} \leq q < (M_{\max} + 1)$ so, here we have the pair $k, k+1 \equiv M_{\max}, (M_{\max} + 1)$. Let now $q \in \mathbb{Q}$ is negative, then $-q$ is positive, then, as we showed above, we can find the pair of integers $k, k+1$ such that $k \leq -q < k+1 \Rightarrow -(k+1) < q < -k$. If $q < -k$, then we have $-(k+1) < q < -k$ and $-(k+1), -k$ is our pair of integers. If $q = -k$, then we have $-k \leq q < -k+1$. And finally, let $q = 0$, then we take $k, k+1 \equiv 0, 1$. The existence is proved.

Uniqueness. Let $k \leq q < k+1$ [1] and $m \leq q < m+1$ [2] here $k \neq m$. Without loss of generality $k < m$, then $m - k$ is a positive (natural) number, so $m - k = \Delta \mid \Delta \in \mathbb{N} \Rightarrow m = k + \Delta$.

Then from [2] we have $k + \Delta \leq q$ and from [1] we have $q < k+1$. Then

$k + \Delta \leq q < k+1 \Rightarrow k + \Delta < k+1 \Rightarrow \Delta < 1$ and we have a contradiction, because $\Delta \in \mathbb{N}$.

The uniqueness is proved.

Let's name the **property5** as “any rational number lies between two integers”.



6

Sequences and limits

Sequences and limits

Def. M is any set and N is a set of natural numbers. Any function $f : N \rightarrow M$ is called a sequence of M , or just a sequence. We will always write x_n instead of $f(n)$ (so, for any concrete $n \in N : f(n) \equiv x_n$). And we will write $\{x_n\}$, or $x_1, x_2, x_3, x_4 \dots$ instead of f .

For any concrete $n \in N$, the element x_n is called an ***n-th*** term of the sequence $\{x_n\}$.

From now on $M \equiv F$, where F is any **ordered field** which contains the field of rational numbers Q as a subfield (in particular, there may be $M \equiv Q$).

Def. Let a is any element of F , for any $\varepsilon > 0 \parallel \varepsilon \in F$ the set $O_\varepsilon(a) \equiv \{x \in F \parallel |x - a| < \varepsilon\}$ is called an ε -neighborhood of a , or just a neighborhood of a . A positive element ε is called a radius of $O_\varepsilon(a)$.

Def. $\{x_n\}$ is a sequence of F . If there exist some element $a \in F$ such that **any** ε -neighborhood $O_\varepsilon(a)$ (of a) contains all the terms of the sequence $\{x_n\}$ starting from some number k , i.e., $O_\varepsilon(a)$ contains all the terms $x_{k+1}, x_{k+2}, x_{k+3}, \dots$, then we say “ $\{x_n\}$ goes to a ”, or “ $\{x_n\}$ has a limit a ”, or “ $\{x_n\}$ converges to a ”, or just “ $\{x_n\}$ converges”, and we write $\{x_n\} \rightarrow a$.

In other words, $\{x_n\} \rightarrow a$ if for any $\varepsilon > 0$ there exist some concrete natural number k (which depends on ε) such that $\forall n > k \Rightarrow x_n \in O_\varepsilon(a)$. The last condition can be rewritten like $\forall n > k \Rightarrow |x_n - a| < \varepsilon$.

The sequence may not have any limit at all, for example the sequence $1, 0, 1, 0, 1, 0 \dots$ does not have any limit in F . When $\{x_n\}$ has no limit, we say “ $\{x_n\}$ diverges”.

Assertion1. If $\{x_n\}$ has some limit a , then this limit is unique.

Proof. Let's assume that it's not true, then there exist some other limit $b \neq a$. Let's fix any neighborhoods of a and b that do not intersect. For example, the neighborhoods $O_\varepsilon(a), O_\varepsilon(b)$ with radiuses $\varepsilon \equiv |b - a|/3$ do not intersect (check it, by using the standard inequality $|x + y| \leq |x| + |y| \forall x, y \in F$). Then $O_\varepsilon(a)$ must contain all the terms of $\{x_n\}$, starting from some number k , and $O_\varepsilon(b)$ must contain all the terms of $\{x_n\}$ starting from some number p , then we have a contradiction. Really, any ***n-th*** term x_n , where $n > k, n > p$, must belong to $O_\varepsilon(a)$ and to $O_\varepsilon(b)$, but these neighborhoods do not intersect. So, any sequence $\{x_n\}$ may have only one limit.

Def. The sequence $\{x_n\}$ is called bounded if there exist some positive $M > 0$ such that $|x_n| < M \parallel \forall n$.

Assertion2. If $\{x_n\}$ converges (has some limit a), then $\{x_n\}$ is bounded.

Proof. So $\{x_n\} \rightarrow a$. Let's fix an arbitrary positive $\varepsilon > 0$, then there exist $k \in \mathbb{N}$ such that all the terms $x_{k+1}, x_{k+2}, x_{k+3}, \dots$ lie in $O_\varepsilon(a)$. And the other terms x_1, x_2, \dots, x_k are not necessary from $O_\varepsilon(a)$, let $V = \max\{|x_1|, |x_2|, \dots, |x_k|, |a| + \varepsilon\}$ so V is the greatest among several non-negative elements which are listed inside the brackets $\{ \dots \}$. Obviously $V > 0$, because $|a| + \varepsilon > 0$. Let's show that for any $x_m \in \{x_n\}$ we have $|x_m| < V + 1$. If x_m is one of the elements x_1, x_2, \dots, x_k , for example $x_m \equiv x_2$, then $|x_m| = |x_2| \leq V < V + 1$. Let x_m is one of the elements $x_{k+1}, x_{k+2}, x_{k+3}, \dots$, then x_m belongs to $O_\varepsilon(a)$, so $|x_m - a| < \varepsilon$, from the standard inequality for absolute value we have:

$$|x_m| - |a| \leq |x_m - a| < \varepsilon \Rightarrow |x_m| < |a| + \varepsilon \leq V < V + 1.$$

So, for any element x_m of our sequence, we have $|x_m| < V + 1$. As $V > 0$, then $V + 1 > 0$.

Let's denote $M \equiv V + 1$, then $|x_m| < M \parallel \forall m$ and the sequence $\{x_n\}$ is bounded, everything is proved.

The converse statement is not true. If $\{x_n\}$ is bounded it may not have any limit.

Example. 1,0,1,0,1,0

Def. Any sequence $\{\alpha_n\}$ which goes to zero ($\{\alpha_n\} \rightarrow 0$) is called an infinitely small.

Auxiliary properties. [A] $\{x_n\} \rightarrow a \Rightarrow$ the sequence $\{\alpha_n\} \equiv \{x_n - a\} \parallel \alpha_n \equiv x_n - a \parallel \forall n$ is infinitely small. And conversely, if some sequence $\{x_n\}$ has the representation $x_n = a + \beta_n \parallel \forall n$, where $\{\beta_n\}$ is an infinitely small sequence, then $\{x_n\} \rightarrow a$.

[B] $\{x_n\}$ is bounded (in particular $\{x_n\}$ converges) and $\{\alpha_n\}$ is infinitely small, then $\{x_n \cdot \alpha_n\}$ is infinitely small.

[C] $\{\alpha_n\}$ and $\{\beta_n\}$ are infinitely small, then $\{\alpha_n + \beta_n\}$ is infinitely small.

[D] If $\{x_n\} \rightarrow a$, then $\{-x_n\} \rightarrow -a$.

[E] $\{x_n\} \rightarrow a$ and $x_n \neq 0 \parallel \forall n$ and $a \neq 0$, then $\left\{ \frac{1}{x_n} \right\} \rightarrow \frac{1}{a}$.

Proof. Let's prove **[A]**. Let we have $\{x_n\} \rightarrow a$. Then, for any $\varepsilon > 0$ there exist

$k \in \mathbb{N} : \forall n > k \Rightarrow |x_n - a| < \varepsilon$, we can rewrite the last inequality

$$|x_n - a| < \varepsilon \Leftrightarrow |(x_n - a) - 0| < \varepsilon \Leftrightarrow |\alpha_n - 0| < \varepsilon.$$

So, we have: for any $\varepsilon > 0$ there exist $k \in \mathbb{N} : \forall n > k : |\alpha_n - 0| < \varepsilon$, by definition it means that $\{\alpha_n\} \rightarrow 0$.

Consequence1. Let $\{x_n\} \rightarrow a$, then the sequence $\{\alpha_n\} \equiv \{x_n - a\}$ is infinitely small and there is a simple representation: $x_n = a + \alpha_n \parallel \forall n$, where $\{\alpha_n\} \rightarrow 0$.

Let now we have some sequence $\{x_n\}$ and the representation $x_n = a + \beta_n \parallel \forall n$, where $\{\beta_n\} \rightarrow 0$. As $\{\beta_n\} \rightarrow 0$, then for any $\varepsilon > 0$ there exist $k \in \mathbb{N} : \forall n > k \Rightarrow |\beta_n| < \varepsilon$. Let's rewrite the last inequality: $|\beta_n| < \varepsilon \Leftrightarrow |(a + \beta_n) - a| < \varepsilon \Leftrightarrow |x_n - a| < \varepsilon$. So, for any $\varepsilon > 0$ there exist $k \in \mathbb{N} : \forall n > k \Rightarrow |x_n - a| < \varepsilon$, by definition it means that $\{x_n\} \rightarrow a$.

Let's prove **[B]**. So, $\exists M > 0$ such that $|x_n| < M \parallel \forall n$. Let's fix an arbitrary positive $\varepsilon > 0$.

Then for the positive element ε / M (as for any other positive element) there exist

$k \in \mathbb{N} : \forall n > k : |\alpha_n - 0| < \varepsilon / M \Leftrightarrow |\alpha_n| < \varepsilon / M$, then $\forall n > k$ we have

$|x_n \cdot \alpha_n - 0| = |x_n \cdot \alpha_n| = |x_n| \cdot |\alpha_n| < M \cdot \varepsilon / M = \varepsilon$. So, for any positive $\varepsilon > 0$ there exist

$k \in \mathbb{N} : \forall n > k \Rightarrow |x_n \cdot \alpha_n - 0| < \varepsilon$, it means that $\{x_n \cdot \alpha_n\}$ is infinitely small.

Consequence2. For any element $a \in F$ and for any infinitely small $\{\alpha_n\}$, the sequence $\{a \cdot \alpha_n\}$ is infinitely small. Really, the sequence $\{x_n\} = a, a, a, \dots$ is a bounded sequence, then $\{x_n \cdot \alpha_n\} = \{a \cdot \alpha_n\}$ is infinitely small. Also: if $\{\alpha_n\}$ and $\{\beta_n\}$ are infinitely small, then $\{\alpha_n \cdot \beta_n\}$ is infinitely small.

Let's prove **[C]**. $\{\alpha_n\} \rightarrow 0$ and $\{\beta_n\} \rightarrow 0$. Let's fix an arbitrary positive $\varepsilon > 0$. For $\varepsilon / 2 > 0$ there exist such $k : \forall n > k$ we have $|\alpha_n - 0| < \varepsilon / 2 \Leftrightarrow |\alpha_n| < \varepsilon / 2$. In the same time for $\varepsilon / 2 > 0$ there exist $p : \forall n > p$ we have $|\beta_n| < \varepsilon / 2$. Let $m = \max(p, k)$, then for any $n > m$ we have $|\alpha_n| < \varepsilon / 2$ and $|\beta_n| < \varepsilon / 2$, then $|(\alpha_n + \beta_n) - 0| = |\alpha_n + \beta_n| \leq |\alpha_n| + |\beta_n| < \varepsilon / 2 + \varepsilon / 2 = \varepsilon$. We have deduced that for any $\varepsilon > 0$ there exist m , such that $\forall n > m$ we have $|(\alpha_n + \beta_n) - 0| < \varepsilon$.

Then $\{\alpha_n + \beta_n\} \rightarrow 0$ and $\{\alpha_n + \beta_n\}$ is infinitely small.

Consequence3. A sum of several infinitely small sequences is again an infinitely small sequence.

Let's prove **[D]**. As $\{x_n\} \rightarrow a$, then for any

$\varepsilon > 0 \exists k \in \mathbb{N} : \forall n > k : |x_n - a| < \varepsilon \Leftrightarrow |(-x_n) - (-a)| < \varepsilon \Rightarrow \{-x_n\} \rightarrow -a$.

Let's prove **[E]**. According to **[A]**, it's enough to prove that the sequence $\left\{ \frac{1}{x_n} - \frac{1}{a} \right\}$ is infinitely

small. Let's rewrite $\left\{ \frac{1}{x_n} - \frac{1}{a} \right\} = \left\{ \frac{a - x_n}{x_n \cdot a} \right\}$. As $\{x_n\} \rightarrow a$, then $\{x_n\}$ is bounded,

let's fix any $M > 0$ such that $|x_n| < M$. We also have $a \neq 0$.

Let $a > 0$, we take the positive $a/2 > 0$. Starting from some number k , all the terms of $\{x_n\}$ lie in $a/2$ -neighborhood of a , so $\exists k \in \mathbb{N} : \forall n > k : |x_n - a| < a/2$.

Then $-a/2 < x_n - a < a/2 \Rightarrow a/2 < x_n < 3a/2$. Let's fix now any positive $\varepsilon > 0$.

We have $\{x_n\} \rightarrow a$, then for the positive number $\varepsilon \cdot a^2/2$ (as for any other positive number) there exist $m \in \mathbb{N} : \forall n > m : |x_n - a| < \varepsilon \cdot a^2/2$. Let's take now the maximal $p \equiv \max(m, k)$, then for any $n > p$ both conditions $a/2 < x_n < 3a/2$ and $|x_n - a| < \varepsilon \cdot a^2/2$ are true.

For any concrete $n > p$, let's estimate:

$$\left| \frac{a - x_n}{x_n \cdot a} - 0 \right| = \left| \frac{a - x_n}{x_n \cdot a} \right| = \frac{|a - x_n|}{|x_n \cdot a|} = \frac{|x_n - a|}{|x_n| \cdot |a|} < \frac{\varepsilon \cdot a^2/2}{|x_n| \cdot a} < \frac{\varepsilon \cdot a^2/2}{a/2 \cdot a} = \varepsilon. \text{ So, we had fixed an}$$

arbitrary positive $\varepsilon > 0$ and we deduced that there exist the number p , such that for any $n > p$

$$\text{we have } \left| \frac{a - x_n}{x_n \cdot a} - 0 \right| < \varepsilon, \text{ it means that } \left\{ \frac{1}{x_n} - \frac{1}{a} \right\} \text{ is infinitely small, then } \left\{ \frac{1}{x_n} \right\} \rightarrow \frac{1}{a}.$$

Let now a is negative, then $a = -|a|$, where $|a|$ is positive. We have $\{x_n\} \rightarrow a \Leftrightarrow \{x_n\} \rightarrow -|a|$, according to [D], we have $\{-x_n\} \rightarrow |a|$, as $|a| > 0$, there must be $\left\{ \frac{1}{-x_n} \right\} \rightarrow \frac{1}{|a|} \Leftrightarrow \left\{ -\frac{1}{x_n} \right\} \rightarrow \frac{1}{|a|}$.

And again, by using [D], we get $\left\{ \frac{1}{x_n} \right\} \rightarrow -\frac{1}{|a|} \Leftrightarrow \left\{ \frac{1}{x_n} \right\} \rightarrow \frac{1}{-|a|} = \frac{1}{a}$, so we have $\left\{ \frac{1}{x_n} \right\} \rightarrow \frac{1}{a}$.

Everything is proved.

Basic properties of convergent sequences. If $\{x_n\} \rightarrow a$ and $\{y_n\} \rightarrow b$, then

$$\text{[1] } \{x_n + y_n\} \rightarrow a + b, \text{ [2] } \{x_n \cdot y_n\} \rightarrow a \cdot b, \text{ [3] if } y_n \neq 0 \ \forall n \text{ and } b \neq 0, \text{ then } \left\{ \frac{x_n}{y_n} \right\} \rightarrow \frac{a}{b}.$$

Proof: We will use the auxiliary properties from above. As $\{x_n\} \rightarrow a$ and $\{y_n\} \rightarrow b$, then the next representations are true: $x_n = a + \alpha_n \parallel \forall n$ and $y_n = b + \beta_n \parallel \forall n$, where $\{\alpha_n\}$ and $\{\beta_n\}$ are infinitely small sequences.

Let's prove [1]. We have $x_n + y_n = (a + b) + (\alpha_n + \beta_n) \parallel \forall n$. According to [C], the sequence $\{\alpha_n + \beta_n\}$ is infinitely small, then (according to [A]) $\{x_n + y_n\} \rightarrow a + b$.

Let's prove [2]. So $x_n \cdot y_n = (a + \alpha_n) \cdot (b + \beta_n) = a \cdot b + (a \cdot \beta_n + \alpha_n \cdot b + \alpha_n \cdot \beta_n)$.

According to [B], all the sequences $\{a \cdot \beta_n\}$, $\{\alpha_n \cdot b\}$, $\{\alpha_n \cdot \beta_n\}$ are infinitely small, then (acc. to [C]), the sequence $\{a \cdot \beta_n + \alpha_n \cdot b + \alpha_n \cdot \beta_n\}$ is infinitely small, then (acc. to [A]) $\{x_n \cdot y_n\} \rightarrow a \cdot b$.

Let's prove [3]. As $y_n \neq 0 \forall n$ and $b \neq 0$ and $\{y_n\} \rightarrow b$, then (acc. to [E]) $\left\{\frac{1}{y_n}\right\} \rightarrow \frac{1}{b}$.

We also have $\{x_n\} \rightarrow a$, then (acc. to [2]) we have $\left\{x_n \cdot \frac{1}{y_n}\right\} \rightarrow a \cdot \frac{1}{b} \Leftrightarrow \left\{\frac{x_n}{y_n}\right\} \rightarrow \frac{a}{b}$.

Consequence4. $\{x_n\} \rightarrow a$ and $\{y_n\} \rightarrow b$, then $\{y_n - x_n\} \rightarrow b - a$. Really, $\{x_n\} \rightarrow a$, then [D] $\{-x_n\} \rightarrow -a$, then (acc. to [1]) $\{y_n + (-x_n)\} \rightarrow b + (-a) \Leftrightarrow \{y_n - x_n\} \rightarrow b - a$.

In particular, a difference of infinitely small sequences is an infinitely small sequence.

Consequence5. Let $\{x_n\} \rightarrow a$ and $\{y_n\} \rightarrow b$. If the sequence $\{y_n\} - \{x_n\} \equiv \{y_n - x_n\}$ is infinitely small, then $a = b$. Really, according to the consequence1, $\{y_n - x_n\} \rightarrow b - a$.

As $\{y_n - x_n\}$ is infinitely small, then $b - a = 0 \Rightarrow b = a$.

Consequence6 (advanced6). $\{y_n\} - \{x_n\} \equiv \{y_n - x_n\}$ is infinitely small. And one of the sequences $\{x_n\}, \{y_n\}$ converges to a , then the other sequence also converges to a . Really, let for example $\{x_n\} \rightarrow a$. Let's denote $\{\alpha_n\} \equiv \{y_n - x_n\}$ (for clarity), then for any n we have the representation $y_n = x_n + \alpha_n$. We know that $\{x_n\} \rightarrow a$ and $\{\alpha_n\} \rightarrow 0$, then from [1] we have: $\{x_n + \alpha_n\} \rightarrow a$ - it is equivalent to $\{y_n\} \rightarrow a$.

Consequence7. Let $\{x_n\} \rightarrow a$, then for any $b \in F$ we have $\{bx_n\} \rightarrow ba$. Really, let's take the sequence $\{y_n\} = b, b, b, b, \dots$. Then (acc. to [2]) $\{x_n \cdot y_n\} = \{x_n \cdot b\} \rightarrow a \cdot b \Leftrightarrow \{bx_n\} \rightarrow ba$.

Let's sum up. We have deduced the basic properties of convergent sequences: $\{x_n\} \rightarrow a$ and $\{y_n\} \rightarrow b$, then $\{x_n \pm y_n\} \rightarrow a \pm b$ and $\{x_n \cdot y_n\} \rightarrow a \cdot b$ and $\{x_n / y_n\} \rightarrow a / b$ (the last one if $y_n \neq 0 \forall n$ and $b \neq 0$). And we can also multiply any convergent sequence by any constant: $\{x_n\} \rightarrow a \Rightarrow \forall b \in F : \{bx_n\} \rightarrow ba$.

Let's consider the set Σ which consists of all infinitely small sequences $\{\alpha_n\}$ of the field F . From the previous results follows that Σ is closed under addition/subtraction/multiplication/multiplication by a constant, i.e., if $\{\alpha_n\}$ and $\{\beta_n\}$ are infinitely small, then $\{\alpha_n \pm \beta_n\}$ and $\{\alpha_n \cdot \beta_n\}$ and $\{b \cdot \alpha_n\} \forall b \in F$ are infinitely small.

We will provide the other set of sequences Ω which has exactly the same properties, the set of all fundamental sequences of F .

Def. A sequence $\{x_n\}$ is called fundamental if for any $\varepsilon > 0$ there exist $k \in \mathbb{N}$ such that $\forall m > k, n > k$ we have $|x_m - x_n| < \varepsilon$.

Def. A sequence $\{x_n\}$ is called a stationary sequence if $\{x_n\} = a, a, a, a, \dots$ for some $a \in F$.

Any stationary sequence is obviously fundamental.

Assertion3. $\{x_n\}$ and $\{y_n\}$ are fundamental sequences, then:

[1] $\{x_n + y_n\}$ is fundamental **[2]** $\{x_n \cdot y_n\}$ is fundamental.

Proof. Let's prove **[1]**. We fix an arbitrary $\varepsilon > 0$. For the positive element $\varepsilon/2 > 0$ there exist $k \in \mathbb{N}$ such that $\forall m, n > k \Rightarrow |x_m - x_n| < \varepsilon/2$. Similarly for $\varepsilon/2 > 0$ there exist $p \in \mathbb{N}$ such that $\forall m, n > p \Rightarrow |y_m - y_n| < \varepsilon/2$. Let's take $v = \max(k, p)$, then for any $n > v$ we have:

$|x_m - x_n| < \varepsilon/2$ and $|y_m - y_n| < \varepsilon/2$. Then for any $n > v$ we have

$$|(x_m + y_m) - (x_n + y_n)| = |(x_m - x_n) + (y_m - y_n)| < |x_m - x_n| + |y_m - y_n| < \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

Then for any positive $\varepsilon > 0$ we can find $v \in \mathbb{N}$ such that for any $n > v$:

$|(x_m + y_m) - (x_n + y_n)| < \varepsilon$ it means exactly that $\{x_n + y_n\}$ is fundamental.

Proof. Let's prove **[2]**. **Auxiliary.** If $\{x_n\}$ is fundamental, then $\{x_n\}$ is bounded.

[step1] Let's fix any $\varepsilon > 0$. Then $\exists k \in \mathbb{N} \forall m, n > k \Rightarrow |x_m - x_n| < \varepsilon$.

Let's fix any number $p > k$, then for any $m > p$ we have $|x_m - x_p| < \varepsilon$ (because anyway, both numbers x_m, x_p are greater than k). Let's take $V = \max\{|x_1|, |x_2|, \dots, |x_p|, |x_p| + \varepsilon\}$.

And let's take any element $x_m \in \{x_n\}$. If x_m is one of the elements x_1, x_2, \dots, x_p ,

then obviously $|x_m| \leq V < V + 1$. If x_m is one of the elements $x_p, x_{p+1}, x_{p+2}, \dots$, then $|x_m - x_p| < \varepsilon$.

Let's use the standart inequality for absolute value: $|x_m| - |x_p| \leq |x_m - x_p| < \varepsilon$, then

$$|x_m| < |x_p| + \varepsilon \Rightarrow |x_m| < V < V + 1.$$

So, for any element $x_m \in \{x_n\}$ we have $|x_m| < V + 1$. Obviously $V > 0 \Rightarrow V + 1 > 0$.

We can denote $M \equiv V + 1$, then $|x_m| < M \parallel \forall m$ and $\{x_n\}$ is a bounded sequence.

[step2] Let now $\{x_n\}$ and $\{y_n\}$ are fundamental, then they are both bounded:

$\exists M > 0: |x_m| < M \parallel \forall m$ and $\exists T > 0: |y_m| < T \parallel \forall m$. Let's take $V = \max(M, T)$, then $|x_m| < V$ and $|y_m| < V$ for any m . Let's fix an arbitrary positive $\varepsilon > 0$. As $\{y_n\}$ is fundamental, for $\varepsilon/V > 0$ there exist $k \in \mathbb{N}: \forall m, n > k \Rightarrow |y_m - y_n| < \varepsilon/2V$. As $\{x_n\}$ is fundamental, for $\varepsilon/V > 0$ there exist $p \in \mathbb{N}: \forall m, n > p \Rightarrow |x_m - x_n| < \varepsilon/2V$. Let's take the number $v \equiv \max(k, p)$, then for any $m, n > v$ we have $|y_m - y_n| < \varepsilon/2V$ and $|x_m - x_n| < \varepsilon/2V$. Then for any $m, n > v$ we have:

$$\begin{aligned} |x_m \cdot y_m - x_n \cdot y_n| &= |(x_m - x_n) \cdot y_m + (y_m - y_n) \cdot x_n| \leq |(x_m - x_n) \cdot y_m| + |(y_m - y_n) \cdot x_n| = \\ &= |x_m - x_n| \cdot |y_m| + |y_m - y_n| \cdot |x_n| < (\varepsilon/2V) \cdot V + (\varepsilon/2V) \cdot V = \varepsilon/2 + \varepsilon/2 = \varepsilon. \end{aligned}$$

Let's sum up: we had started from an arbitrary positive $\varepsilon > 0$, and we showed that there exist some number v , such that $\forall m, n > v$ we have $|x_m \cdot y_m - x_n \cdot y_n| < \varepsilon$, it means that $\{x_n \cdot y_n\}$ is fundamental.

Consequence8. If $\{x_n\}$ is fundamental, then for any $b \in F$ the sequence $\{b \cdot x_n\}$ is fundamental. Really, let's take the stationary sequence $\{y_n\} = b, b, b, b \dots$ (this sequence is fundamental), then (according to [2]) $\{x_n \cdot y_n\} = \{bx_n\}$ is fundamental.

Consequence9. If $\{x_n\}$ and $\{y_n\}$ are fundamental, then $\{x_n\} - \{y_n\} \equiv \{x_n - y_n\}$ is fundamental. Really, as $\{y_n\}$ is fundamental, then (**consequence8** $b = -1 \in Q \subset F$) the sequence $\{-y_n\}$ is fundamental. Then (according to [1]) $\{x_n + (-y_n)\} = \{x_n - y_n\}$ is fundamental.

Let's sum up. The set Ω of all fundamental sequences of F is closed under addition/subtraction/multiplication/multiplication by a constant, i.e, if $\{x_n\}$ and $\{y_n\}$ are fundamental, then $\{x_n \pm y_n\}, \{x_n \cdot y_n\}, \{bx_n\} \forall b \in F$ are fundamental.

Assertion4. If $\{x_n\}$ converges (to some limit a), then $\{x_n\}$ is fundamental.

Proof. Let $\{x_n\} \rightarrow a$. We fix an arbitrary $\varepsilon > 0$, then for $\varepsilon/2 > 0$ there exist $k \in \mathbb{N}$ such that $n > k \Rightarrow |x_n - a| < \varepsilon/2$. Then for any $m, n > k$ we have:

$|x_m - x_n| = |(x_m - a) + (a - x_n)| \leq |x_m - a| + |a - x_n| < \varepsilon/2 + \varepsilon/2 = \varepsilon$, then $\{x_n\}$ is a fundamental sequence.

Let's remind. All the results, that we got above, are related to sequences of a field F .

Where F is any ordered field which contains the field of rational numbers Q as a subfield.

(In particular, all this theory is applicable for $F = Q$). The existence of an ordered field

$F \supset Q \parallel F \neq Q$ is still under a question. We still haven't built yet any example of such field F , but when we do, we will be able to use in F all these results.

Let's look at the **assertion4**. The next question has a **great importance** in math:

“If $\{x_n\}$ is fundamental in F , does it converge to some $a \in F$?” **[Q]**.

The general answer is “no”, or better “not necessary”. In general, it depends on the field F and on the concrete sequence $\{x_n\}$ of F . But we are not interested in such randomness, we want to work only in such fields, where the answer on **[Q]** is “Yes”. And we will build the **complete fields** R, C , where the answer is always “Yes”.

Def. A field F is called a **complete field** if any fundamental sequence $\{x_n\}$ of F converges in F .

Notice, the field of rational numbers Q is not a complete field. There are sequences of rational numbers which are fundamental, but do not have any limit in Q . It's much more convenient to provide examples of such sequences after construction of the field of real numbers $R \supset Q$.

Squeeze Theorem for sequences. Let $\{x_n\}, \{y_n\}, \{z_n\}$ are some sequences of F .

Starting from some number k we have $x_n \leq y_n \leq z_n \parallel \forall n > k$.

And both sequences $\{x_n\}, \{z_n\}$ go to the same limit a , then $\{y_n\}$ also goes to a .

Auxiliary assertion. There are positive sequences $\{\alpha_n\}, \{\beta_n\}$ and $0 \leq \alpha_n \leq \beta_n \parallel \forall n$.

If $\{\beta_n\}$ is infinitely small, then $\{\alpha_n\}$ is infinitely small.

Proof. $\forall \varepsilon > 0 \exists k, \forall n > k \Rightarrow |\beta_n| < \varepsilon$. From $0 \leq \alpha_n \leq \beta_n$ immediately follows that $|\alpha_n| \leq |\beta_n|$.

Then $\forall \varepsilon > 0 \exists k, \forall n > k \Rightarrow |\beta_n| < \varepsilon \Rightarrow |\alpha_n| < \varepsilon$, so $\{\alpha_n\}$ is infinitely small.

Comment. Let's notice a very important moment. From any sequence $\{x_n\}$ we can discard any finite amount of its first consecutive terms $x_1, x_2, x_3 \dots x_k$, it does not affect fundamentality and convergence. Let's explain it, when we say that we discard $x_1, x_2, x_3 \dots x_k$ from $\{x_n\}$, we mean that we consider the new sequence $\{\tilde{x}_n\} \parallel \tilde{x}_1 \equiv x_{k+1}, \tilde{x}_2 \equiv x_{k+2}, \tilde{x}_3 \equiv x_{k+3}, \dots$

It's very easy to understand that: $\{x_n\}$ is fundamental $\Leftrightarrow \{\tilde{x}_n\}$ is fundamental.

And: $\{x_n\}$ converges to $a \Leftrightarrow \{\tilde{x}_n\}$ converges to a . This great idea will be used several times during the construction of real numbers.

Let's prove now the **squeeze theorem**. We can obviously discard all the terms of the sequences with numbers $1, 2, 3 \dots k$ (it will not affect convergence), then we can assume that from the very beginning we have $x_n \leq y_n \leq z_n \parallel \forall n$. Let's subtract x_n from all sides, then $0 \leq y_n - x_n \leq z_n - x_n$.

Let $(z_n - x_n) \equiv \beta_n$ and $(y_n - x_n) \equiv \alpha_n$, then we have $0 \leq \alpha_n \leq \beta_n$. As $\{x_n\} \rightarrow a$ and $\{z_n\} \rightarrow a$, then (**consequence4**) $\{z_n - x_n\} \rightarrow 0 \Leftrightarrow \{\beta_n\} \rightarrow 0$, then (**auxiliary assertion** above)

$\{\alpha_n\} \rightarrow 0 \Leftrightarrow \{y_n - x_n\} \rightarrow 0$. As $\{x_n\} \rightarrow a$, then (**consequence6**) $\{y_n\} \rightarrow a$.

Def. F is an ordered field. If the **Archimedes axiom** is true in F , then we say “ F is an Archimedean ordered field”.

Comment. The next chapter is dedicated to the construction of real numbers. If we write $\{q_n\} \subset Q$, we mean that we have a sequence of rational numbers $\{q_n\}$. This writing is used because it's convenient. But normally, the symbol \subset is used to show that one set belongs to the other.

In our case Q is a set, but $\{q_n\}$ is not a set, it is a function! $f: \mathbb{N} \rightarrow Q$ (look at the definition of a sequence, **page 85**). And numbers $q_1, q_2, q_3, q_4 \dots$ are only values of that function.

So, if someone wants to avoid misunderstanding, it's better to write $\{q_n\} \parallel q_n \in Q, \forall n$, or to make an explanation of a new writing, like we just did.



7

*Real
numbers*

Pre-real numbers

As earlier, F is an ordered field which contains the field Q as a subfield. We will prove the auxiliary theorem that will help us in the construction process.

Obviously, if some sequence $\{q_n\} \subset Q \subset F$ is fundamental in F , then $\{q_n\}$ is fundamental in Q .

Really: $\{q_n\}$ is fundamental in F , then $\forall \varepsilon \in F \parallel \varepsilon > 0 \exists k : \forall m, n > k \Rightarrow |x_m - x_n| < \varepsilon$.

Then a fortiori $\forall \varepsilon \in Q \parallel \varepsilon > 0 \exists k : \forall m, n > k \Rightarrow |x_m - x_n| < \varepsilon$ (because $Q \subset F$).

The converse assertion in general is not true, if $\{q_n\} \subset Q \subset F$ is fundamental in Q , it mustn't be fundamental in F .

And similarly, if $\{q_n\} \subset Q \subset F$ converges to some $q \in Q$ as a sequence of F , then it converges to q as a sequence of Q . And again, the converse assertion is not true.

If $\{q_n\} \subset Q$ converges to some $q \in Q$ as a sequence of Q , it mustn't converge to q as a sequence of F (obviously, there can be only two variants, either $\{q_n\}$ does not converge in F , or $\{q_n\}$ converges in F , and in this case, of course, $\{q_n\}$ converges in F to the same $q \in Q$).

Theorem 1. The **Archimedes axiom** is true in F . Then:

[A] Every sequence $\{q_n\} \subset Q$ that converges/fundamental in Q also converges/fundamental in F .

[B] Every element $a \in F$ can be represented as a limit of some rational sequence $\{q_n\} \subset Q$.

Proof. Let's fix an arbitrary sequence $\{q_n\} \subset Q$ which is fundamental in Q . Let's fix an **arbitrary** positive $\varepsilon \in F$. We want to show that $\exists k \in \mathbb{N} : \forall m, n > k \Rightarrow |x_m - x_n| < \varepsilon$. Both elements 1, $1/\varepsilon$ are positive, according to the **Archimedes axiom**, there exist $\tilde{k} \in \mathbb{N}$ such that

$\tilde{k} \cdot 1 > 1/\varepsilon \Rightarrow \tilde{k} \cdot \varepsilon > 1 \Rightarrow \varepsilon > 1/\tilde{k} \in Q$. As $\{q_n\}$ is fundamental in Q , for the rational number $1/\tilde{k} > 0$, there exist $k \in \mathbb{N} : \forall m, n > k \Rightarrow |x_m - x_n| < 1/\tilde{k}$, then $\forall m, n > k \Rightarrow |x_m - x_n| < \varepsilon$.

So $\{q_n\}$ is fundamental in F .

Let's fix an arbitrary sequence $\{q_n\} \subset Q$ which converges in Q to some element $q \in Q$.

Let's fix an **arbitrary** positive $\varepsilon \in F$. We want to show that $\exists k \in \mathbb{N} : \forall n > k \Rightarrow |x_n - q| < \varepsilon$.

In the same way as above, we will find the positive rational number $1/\tilde{k}$ such that $1/\tilde{k} < \varepsilon$.

As $\{q_n\} \rightarrow q$ in Q , there exist $\exists k \in \mathbb{N} : \forall n > k \Rightarrow |x_n - q| < 1/\tilde{k}$, then $\forall n > k \Rightarrow |x_n - q| < \varepsilon$.

So $\{q_n\} \rightarrow q$ in F . And **[A]** is proved.

Let's prove **[B]**. The proof here will be a bit more voluminous than usually, but we will build here a very important example which we will use in the future in the "Length construction".

As this example is important for us, we name it an **[Example L]**.

Let's fix an arbitrary **positive** $a \in F$, there exist $n \in \mathbb{N}$ such that $1/n < a$ (we have shown it above, there was an arbitrary positive ε instead of a).

The set X of natural numbers m such that $m/n \leq a$ is not empty (it contains $m=1$), in the same time, there exist the natural number k such that $k \cdot 1/n = k/n > a$ (the **Archimedes axiom** for $1/n, a$).

Then X has the greatest number $m_0^{\max} \in X$. Then $m_0^{\max}/n \leq a < (m_0^{\max} + 1)/n$.

Let's sum up: $m_0^{\max} \equiv T_0$ is the greatest natural number such that $T_0/n \leq a$ and $m_0^{\max} + 1 \equiv M_0$ is the least natural number such that $a < M_0/n$ and $T_0 + 1 = M_0$. So $\frac{T_0}{n} \leq a < \frac{M_0}{2n} \parallel L_0 + 1 = M_0$.

Let's consider all the possible fractions $\left\{ \frac{1}{2^k n} \parallel k \in \mathbb{N} \right\}$. Each of these fractions is less than the

initial fraction $\frac{1}{n}$ (from above) and therefore each fraction is less than a . In exactly the same way

as above, for each fraction $\frac{1}{2^k n}$ there exist the pair of natural numbers T_k, M_k such that

$$\frac{T_k}{2^k n} \leq a < \frac{M_k}{2^k n} \parallel T_k + 1 = M_k. \text{ Let's notice: [At first] For any integer } k \geq 0 \text{ we have } \frac{T_k}{2^k n} \leq \frac{T_{k+1}}{2^{k+1} n}.$$

Really, $\frac{T_k}{2^k n} = \frac{2 \cdot T_k}{2 \cdot 2^k n} = \frac{2T_k}{2^{k+1} n} \leq a$ we know that T_{k+1} is the greatest among all the natural numbers

m , for which $\frac{m}{2^{k+1} n} \leq a$, then of course $2T_k \leq T_{k+1}$ and as a consequence,

$$\frac{2T_k}{2^{k+1} n} \leq \frac{T_{k+1}}{2^{k+1} n} \Leftrightarrow \frac{T_k}{2^k n} \leq \frac{T_{k+1}}{2^{k+1} n}.$$

[Secondly] For any integer $k \geq 0$ we have $\frac{M_{k+1}}{2^{k+1} n} \leq \frac{M_k}{2^k n}$. Really, $\frac{M_k}{2^k n} = \frac{2 \cdot M_k}{2 \cdot 2^k n} = \frac{2M_k}{2^{k+1} n} > a$ and

we know that M_{k+1} is the least among all the natural numbers m , for which $\frac{m}{2^{k+1} n} > a$,

then, of course, $2M_k \geq M_{k+1}$ and as a consequence $\frac{2M_k}{2^{k+1} n} \geq \frac{M_{k+1}}{2^{k+1} n} \Leftrightarrow \frac{M_k}{2^k n} \geq \frac{M_{k+1}}{2^{k+1} n}$.

So, we have: $\frac{T_0}{n} \leq \frac{T_1}{2n} \leq \frac{T_2}{2^2 n} \leq \frac{T_3}{2^3 n} \leq \dots \leq a < \dots \leq \frac{M_3}{2^3 n} \leq \frac{M_2}{2^2 n} \leq \frac{M_1}{2n} \leq \frac{M_0}{n}$ which is equivalent to

$$\frac{T_0}{n} \leq \frac{T_1}{2n} \leq \frac{T_2}{2^2 n} \leq \frac{T_3}{2^3 n} \leq \dots \leq a < \dots \leq \frac{T_3 + 1}{2^3 n} \leq \frac{T_2 + 1}{2^2 n} \leq \frac{T_1 + 1}{2n} \leq \frac{T_0 + 1}{n} \text{ [E]. The sequence } \left\{ \frac{T_k}{2^k n} \right\} \text{ is}$$

obviously a sequence of rational numbers, let's show that it converges to a . From [E] we have

$$\frac{T_k}{2^k n} \leq a < \frac{T_k + 1}{2^k n} \parallel \forall k \geq 0.$$

Let's subtract $\frac{T_k}{2^k n}$ from all sides, then $0 \leq a - \frac{T_k}{2^k n} < \frac{T_k + 1}{2^k n} - \frac{T_k}{2^k n} \Rightarrow$ for any integer $k \geq 0$ we have $0 \leq a - \frac{T_k}{2^k n} < \frac{1}{2^k n}$. We can apply here the **squeeze theorem for sequences**.

Really, let's consider $\{x_k\} \equiv 0, 0, 0, 0, 0, \dots$ and $\{y_k\} \equiv \left\{a - \frac{T_k}{2^k n}\right\}$ and $\{z_k\} \equiv \left\{\frac{1}{2^k n}\right\}$ we have $x_k \leq y_k \leq z_k \parallel \forall k$ and obviously $\{x_k\} \rightarrow 0$ (in F). The rational sequence $\{z_k\}$ obviously converges to zero in Q , then (according to [A]) it converges to zero in $F \supset Q$. So both $\{x_k\} \rightarrow 0$, $\{z_k\} \rightarrow 0$, then (the **squeeze theorem for sequences**) $\{y_k\} \rightarrow 0$.

So, the sequence $\left\{a - \frac{T_k}{2^k n}\right\}$ is infinitely small, then $\left\{\frac{T_k}{2^k n}\right\} \rightarrow a$, where $\left\{\frac{T_k}{2^k n}\right\} \subset Q$ and a is an arbitrary positive element of F . So, any positive $a \in F$ can be represented as a limit of some rational sequence. Let a is negative, then $a = -|a|$ where $|a|$ is positive, therefore there exist some $\{q_n\} \subset Q \parallel \{q_n\} \rightarrow |a|$, then $\{-q_n\} \rightarrow -|a| \Leftrightarrow \{-q_n\} \rightarrow a$ and $\{-q_n\} \subset Q$.

And finally, let $a = 0$, then a can be represented as a limit of the rational sequence $\{0\} \equiv 0, 0, 0, 0, \dots$,

or as a limit of the rational sequence $\left\{\frac{1}{n}\right\} \equiv 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots$, or as a limit of

$\left\{-\frac{1}{n}\right\} \equiv -1, -\frac{1}{2}, -\frac{1}{3}, -\frac{1}{4}, \dots$. Everything is proved.

The Reader could notice that for any element $a \in F$ it's representation as a limit of some rational sequence is not unique (we have shown it only for $0 \in F$). Really, let's fix any $a \in F$.

We shown above that there exist at least one rational sequence $\{q_n\} \rightarrow a$. Let's take the sequence

$\left\{\frac{1}{n}\right\} \rightarrow 0$, then $\left\{q_n + \frac{1}{n}\right\} \rightarrow a + 0 = a$. So, the rational sequence $\left\{q_n + \frac{1}{n}\right\}$ also goes to a

(and it differs from $\{q_n\}$) and similarly $\left\{q_n - \frac{1}{n}\right\} \rightarrow a$.

Real numbers

Def. The complete, Archimedean ordered field R , which contains the field Q of rational numbers as a subfield, is called a field of real numbers. Elements of R are called real numbers.

The addition and multiplication on R are extensions of the addition and multiplication on Q , i.e., for any $a, b \in Q \subset R$:

$a + b$ (addition by the rules of R) = $a + b$ (addition by the rules of Q),

$a \cdot b$ (multiplication by the rules of R) = $a \cdot b$ (multiplication by the rules of Q).

Let's build R . We fix any set Q of rational numbers. Let's consider the set Ω of all fundamental sequences $\{q_n\}$ of rational numbers. We define addition and multiplication on Ω .

Def. $\forall \{q_n\}, \{p_n\} \in \Omega \Rightarrow \{q_n\} + \{p_n\} \equiv \{q_n + p_n\}$ and $\{q_n\} \cdot \{p_n\} \equiv \{q_n \cdot p_n\}$. We showed earlier that the set Ω of all fundamental sequences is closed under addition and multiplication, so if $\{q_n\}, \{p_n\}$ are fundamental, then $\{q_n + p_n\}$ and $\{q_n \cdot p_n\}$ are also fundamental, therefore these sequences belong to Ω .

We have defined the addition "+" and multiplication "." on Ω , these operations are associative and commutative (because the addition and multiplication of rational numbers are associative and commutative). There is also a distributive law: $(\{p_n\} + \{q_n\}) \cdot \{h_n\} = \{p_n\} \cdot \{h_n\} + \{q_n\} \cdot \{h_n\}$ and $\{h_n\} \cdot (\{p_n\} + \{q_n\}) = \{h_n\} \cdot \{p_n\} + \{h_n\} \cdot \{q_n\}$ [D] which immediately follows from the distributive law for rational numbers.

Def. Sequences $\{q_n\}, \{p_n\} \in \Omega$ are equivalent $\{q_n\} \approx \{p_n\}$ if the sequence $\{q_n - p_n\}$ is infinitely small. Such relation \approx on Ω is obviously reflexive, symmetric, transitive. So, \approx is an equivalence relation on Ω . Then \approx divides Ω into the classes $A, B, C, D \dots$ of equivalent (fundamental) sequences. The set of all classes we denote like R_{aux} .

Let's define addition and multiplication on R_{aux} in order to turn R_{aux} into a field.

Def. For any $A, B \in R_{aux}$: if $\{q_n\} \in A$ and $\{p_n\} \in B$, then $A + B$ is the class which contains the sequence $\{q_n + p_n\}$. And $A \cdot B$ is the class which contains the sequence $\{q_n \cdot p_n\}$. As sum and product of any fundamental sequences $\{q_n\}, \{p_n\}$ are again fundamental sequences, the classes $A + B$ and $A \cdot B$ do exist.

Let's show that these classes are uniquely defined. Let $\{q_n\}, \{\bar{q}_n\} \in A$ and $\{p_n\}, \{\bar{p}_n\} \in B$ we need to show that $\{q_n\} + \{p_n\} \approx \{\bar{q}_n\} + \{\bar{p}_n\}$ and $\{q_n\} \cdot \{p_n\} \approx \{\bar{q}_n\} \cdot \{\bar{p}_n\}$. So, as $\{q_n\}, \{\bar{q}_n\} \in A$, then $\{q_n - \bar{q}_n\} \equiv \{\alpha_n\}$ (an infinitely small sequence), then $q_n - \bar{q}_n = \alpha_n \forall n \Rightarrow q_n = \bar{q}_n + \alpha_n$ and similarly $\{p_n - \bar{p}_n\} \equiv \{\beta_n\}$ (an infinitely small sequence), then $p_n - \bar{p}_n = \beta_n \forall n \Rightarrow p_n = \bar{p}_n + \beta_n$.

The sequences $\{q_n + p_n\}$ and $\{\bar{q}_n + \bar{p}_n\}$ are equivalent if the sequence $\{(q_n + p_n) - (\bar{q}_n + \bar{p}_n)\}$

is infinitely small. So, $\{(q_n + p_n) - (\bar{q}_n + \bar{p}_n)\} = \{(\bar{q}_n + \alpha_n + \bar{p}_n + \beta_n) - (\bar{q}_n + \bar{p}_n)\} = \{\alpha_n + \beta_n\}$, the last sequence is infinitely small, because $\{\alpha_n\}$ and $\{\beta_n\}$ are infinitely small.

Next, the sequences $\{q_n \cdot p_n\}$ and $\{\bar{q}_n \cdot \bar{p}_n\}$ are equivalent if the sequence $\{q_n \cdot p_n - \bar{q}_n \cdot \bar{p}_n\}$ is infinitely small. So, $\{q_n \cdot p_n - \bar{q}_n \cdot \bar{p}_n\} = \{(\bar{q}_n + \alpha_n) \cdot (\bar{p}_n + \beta_n) - \bar{q}_n \cdot \bar{p}_n\} = \{\bar{q}_n \cdot \beta_n + \alpha_n \cdot \bar{p}_n + \alpha_n \cdot \beta_n\}$ the last sequence is infinitely small. Really, $\{\bar{q}_n\}$ is fundamental and therefore it is bounded, the product of any bounded and infinitely small sequence is an infinitely small sequence, then $\{\bar{q}_n \cdot \beta_n\}$ is infinitely small. Similarly $\{\alpha_n \cdot \bar{p}_n\}$ is infinitely small, and also $\{\alpha_n \cdot \beta_n\}$ is infinitely small. Then $\{\bar{q}_n \cdot \beta_n + \alpha_n \cdot \bar{p}_n + \alpha_n \cdot \beta_n\}$ is infinitely small, everything is proved.

Now we have the set of classes R_{aux} with two operations $+$, \cdot on it.

Assertion1. $(R_{aux}, +, \cdot)$ is a field.

Proof. The addition of sequences is associative and commutative, therefore, the addition of classes is associative and commutative on R_{aux} . The zero class O is the class which contains the sequence $\{0\} \equiv 0, 0, 0, 0, \dots$, it consists of all infinitely small sequences of rational numbers.

Really, let $\{\alpha_n\} \in O$, then $\{\alpha_n\} \approx \{0\}$, then $\{\alpha_n - 0\}$ is infinitely small, then $\{\alpha_n\}$ is infinitely small. Conversely, let $\{\alpha_n\}$ is infinitely small, then $\{\alpha_n - 0\}$ is infinitely small, then $\{\alpha_n\} \approx \{0\}$, then $\{\alpha_n\} \in O$. Next, for any class A which contains a sequence $\{q_n\}$, an opposite class $-A$ is the class which contains the sequence $\{-q_n\}$.

The multiplication of sequences is associative, then the multiplication of classes is also associative. And finally, there is a distributive law **[D]**, then there is the same distributive law for classes. So R_{aux} is a ring.

Let's show that $R_{aux} \setminus O$ is commutative multiplicative group. We need to show that $R_{aux} \setminus O$ is closed under multiplication (or it's not a multiplicative group). In order to do that, we need to derive several important auxiliary facts.

Auxiliary1. For any class $A \neq O$ only one of the next cases is true: **[A]** or **[B]**.

[A] There exist the positive rational number ρ and the sequence $\{q_n\} \in A$ such that $\rho < q_n \parallel \forall n$.

[B] There exist the negative rational number η and the sequence $\{q_n\} \in A$ such that $q_n < \eta \parallel \forall n$.

Let's fix an arbitrary sequence $\{q_n\} \in A \neq O$, we will get the needed sequence from it, by using only two conditions: $\{q_n\}$ is **not** an infinitely small and $\{q_n\}$ is fundamental.

Let's explain. The zero class consists of all infinitely small sequences of rational numbers, as $\{q_n\} \notin O$, then $\{q_n\}$ is not an infinitely small. If some sequence $\{x_n\}$ is infinitely small, it means that $\forall \varepsilon > 0 \exists k, \forall n > k \Rightarrow |x_n| < \varepsilon$. As $\{q_n\}$ is **not** an infinitely small, then there exist some concrete $\bar{\varepsilon} > 0$, for which the requirement $\exists k, \forall n > k \Rightarrow |q_n| < \bar{\varepsilon}$ is **not** true, so for any natural number k

there exist at least one natural number $\bar{n} > k$ such that $|q_{\bar{n}}| \geq \bar{\varepsilon}$.

Let's sum up: $\exists \bar{\varepsilon} > 0 : \forall k \exists \bar{n} > k \Rightarrow |q_{\bar{n}}| \geq \bar{\varepsilon}$. We fix now this concrete positive $\bar{\varepsilon}$.

Let's remember now that $\{q_n\}$ (which is fixed above) is fundamental, so for the number $\bar{\varepsilon}/2 > 0$ we can fix the number \bar{k} such that for any $m, n > \bar{k}$ we have $|q_m - q_n| < \bar{\varepsilon}/2$ [F].

As we noticed above, we can fix some concrete $\bar{n} > \bar{k}$ such that $|q_{\bar{n}}| \geq \bar{\varepsilon}$. Then for any natural number $m > \bar{k}$ we have $m, \bar{n} > \bar{k}$ and therefore: $|q_m - q_{\bar{n}}| < \bar{\varepsilon}/2$, $|q_{\bar{n}}| \geq \bar{\varepsilon} \Leftrightarrow |q_{\bar{n}} - q_m| < \bar{\varepsilon}/2$, $|q_{\bar{n}}| \geq \bar{\varepsilon}$.

Let's use the inequality $|q_{\bar{n}}| - |q_m| \leq |q_{\bar{n}} - q_m|$, then

$|q_{\bar{n}}| - |q_m| < \bar{\varepsilon}/2$, $|q_{\bar{n}}| \geq \bar{\varepsilon} \Rightarrow |q_{\bar{n}}| - \bar{\varepsilon}/2 < |q_m|$, $|q_{\bar{n}}| \geq \bar{\varepsilon} \Rightarrow \bar{\varepsilon} - \bar{\varepsilon}/2 < |q_m| \Rightarrow \bar{\varepsilon}/2 < |q_m|$ for any $m > \bar{k}$.

So, the **absolute value** of every term $q_{\bar{k}+1}, q_{\bar{k}+2}, q_{\bar{k}+3} \dots$ is greater than $\bar{\varepsilon}/2$.

Let's show that only one of the next cases is true:

[First] Every term $q_{\bar{k}+1}, q_{\bar{k}+2}, q_{\bar{k}+3} \dots$ is greater than $\bar{\varepsilon}/2$.

[Second] Every term $q_{\bar{k}+1}, q_{\bar{k}+2}, q_{\bar{k}+3} \dots$ is less than $-\bar{\varepsilon}/2$.

Really, the absolute value of every term is greater than $\bar{\varepsilon}/2$. So, for any concrete term q_m , where $m > \bar{k}$, we have the case **[First]**, or the case **[Second]**, because from $\bar{\varepsilon}/2 < |q_m|$ follows that either $\bar{\varepsilon}/2 < q_m$, or $q_m < -\bar{\varepsilon}/2$. Let's assume that for some $m, n > \bar{k}$ we have the next situation: $\bar{\varepsilon}/2 < q_m$ and $q_n < -\bar{\varepsilon}/2$ [D]. Then $q_m - q_n > \bar{\varepsilon} \Rightarrow |q_m - q_n| > \bar{\varepsilon}$ which contradicts to [F].

So, for any $m, n > \bar{k}$ there can't be the situation [D]. Then there can be only the case **[First]**, or the case **[Second]**, and no other variants.

Let we have the case **[First]**. Then all the "initial" terms $q_1, q_2 \dots q_{\bar{k}}$ of our sequence we replace by the positive number $\bar{\varepsilon}$. Then we have the sequence $\{\bar{q}_n\} \equiv \bar{\varepsilon}, \bar{\varepsilon} \dots \bar{\varepsilon}, q_{\bar{k}+1}, q_{\bar{k}+2}, q_{\bar{k}+3} \dots$

This sequence is obviously equivalent to $\{q_n\}$ (really, the sequence $\{\bar{q}_n - q_n\}$ is infinitely small, because all it's terms, starting from the number \bar{k} , are zeroes), then $\{\bar{q}_n\} \in A$. And we have the sequence $\{\bar{q}_n\} \in A \parallel \bar{q}_n > \bar{\varepsilon}/2 \forall n$ (it is exactly the case [A] of [auxiliary1](#)).

Let we have the case **[Second]**. Then we replace all the initial terms $q_1, q_2 \dots q_{\bar{k}}$ by the negative number $-\bar{\varepsilon}$, we will get the sequence $\{\bar{q}_n\} \equiv -\bar{\varepsilon}, -\bar{\varepsilon} \dots -\bar{\varepsilon}, q_{\bar{k}+1}, q_{\bar{k}+2}, q_{\bar{k}+3} \dots$ which is equivalent to $\{\bar{q}_n\}$ (and therefore $\{\bar{q}_n\} \in A$). So $\{\bar{q}_n\} \in A \parallel \bar{q}_n < -\bar{\varepsilon}/2 \forall n$ (it is exactly the case [B] of [auxiliary1](#)).

Consequence1. We can unite the cases [A] and [B] in one. For any class $A \neq O$ there exist the positive rational number Δ and the sequence $\{q_n\} \in A$ such that $\Delta < |q_n| \parallel \forall n$.

Auxiliary2. If a rational sequence $\{q_n\} \parallel q_n \neq 0 \ \forall n$ is fundamental and $\Delta < |q_n| \parallel \forall n$, then $\{1/q_n\}$ is also fundamental.

Proof. Let's fix an arbitrary positive $\varepsilon > 0$. For the positive number $\varepsilon \cdot \Delta^2$ (as for any other positive number) there exist $k : \forall m, n > k \Rightarrow |q_m - q_n| < \varepsilon \cdot \Delta^2$. Then for any $m, n > k$ we have

$$\left| \frac{1}{q_m} - \frac{1}{q_n} \right| = \left| \frac{q_n - q_m}{q_m \cdot q_n} \right| = \frac{|q_m - q_n|}{|q_m| \cdot |q_n|} < \frac{\varepsilon \cdot \Delta^2}{|q_m| \cdot |q_n|} < \frac{\varepsilon \cdot \Delta^2}{\Delta \cdot \Delta} = \varepsilon. \text{ Then } \{1/q_n\} \text{ is fundamental.}$$

Let's show now that $R_{aux} \setminus O$ is closed under multiplication. We take any classes $A, B \in R_{aux} \setminus O$.

According to the [consequence1](#), we can take the sequence $\{q_n\} \in A$ such that $\rho < |q_n| \parallel \forall n$ for some $\rho > 0$. And similarly, we can take some $\{p_n\} \in B$ such that $\Delta < |p_n| \parallel \forall n$. Then for the sequence $\{q_n \cdot p_n\} \in A \cdot B$ we have $\rho \cdot \Delta < |q_n \cdot p_n| \parallel \forall n$. Then $\{q_n \cdot p_n\}$ is not an infinitely small.

Then $A \cdot B \neq O \Rightarrow A \cdot B \in R_{aux} \setminus O$.

As the multiplication of sequences is associative and commutative, the multiplication of classes is associative and commutative on all R_{aux} . The set $R_{aux} \setminus O$ is closed under multiplication, then the multiplication of classes is associative and commutative on $R_{aux} \setminus O$.

A class "one" $I \in R_{aux} \setminus O$ is obviously the class which contains the sequence $\{1\} \equiv 1, 1, 1 \dots$

Let's fix any class $A \in R_{aux} \setminus O$, and we take the sequence $\{q_n\} \in A$ such that $\rho < |q_n| \parallel \forall n$ for some $\rho > 0$. The sequence $\{1/q_n\}$ is also fundamental ([auxiliary2](#)) and therefore, it belongs to some class B . The class $A \cdot B$ contains the sequence $\{q_n\} \cdot \{1/q_n\} = \{1\} = 1, 1, 1, \dots$, then $A \cdot B = I$ and similarly $B \cdot A = I$, then, by definition $B = A^{-1}$. Notice that we haven't shown that $A^{-1} \in R_{aux} \setminus O$, which is a very important requirement. Let's assume the contrary: $A^{-1} \notin R_{aux} \setminus O \Rightarrow A^{-1} = O$.

Then the sequence $\{1/q_n\} \in A^{-1}$ is infinitely small, then $\forall \varepsilon > 0 \ \exists k : \forall n > k \Rightarrow |1/q_n| < \varepsilon$, the last inequality is equivalent to $|1/\varepsilon| < |q_n| \Leftrightarrow 1/\varepsilon < |q_n|$. So, for any positive rational $\varepsilon > 0$ we have $1/\varepsilon < |q_n|$, starting from some moment. From here immediately follows that $\{q_n\}$ is not bounded. Really, let's fix any $M > 0$, then for the positive $\varepsilon \equiv 1/M > 0$, the absolute values of terms of $\{q_n\}$ are greater than $1/\varepsilon = M$ (starting from some moment), then $\{q_n\}$ is not bounded. As $\{q_n\}$ is not bounded, it can't be fundamental, and we have a contradiction.

Then $A^{-1} \in R_{aux} \setminus O$ and $R_{aux} \setminus O$ is a commutative group under multiplication. And R_{aux} is a field.

Def: a class A is called positive if there exist some positive rational $\rho > 0$ and the sequence $\{q_n\} \in A$ such that $\rho < q_n \parallel \forall n$.

Assertion2. R_{aux} is an ordered field.

Proof. We need to show that for any $A \in R_{aux}$ only one of the next cases is true: A is positive, $-A$ is positive, $A = O$. Let's take an arbitrary $A \in R_{aux}$. If $A = O$, then any sequence $\{q_n\} \in A$ is infinitely small and there can't be any positive $\rho > 0$ such that $\rho < q_n \parallel \forall n$, so A is not a positive class. The class $-A$ in this case is also a zero class O , so it can't be positive for the same reason. If $A \neq O$, then (according to the [auxiliary1](#)) there can be exactly one case: **[A]** or **[B]**.

[A] There exist the positive rational number ρ and the sequence $\{q_n\} \in A$ such that $\rho < q_n \parallel \forall n$. In this case A is positive. **[B]** There exist the negative rational number η and the sequence $\{q_n\} \in A$ such that $q_n < \eta \parallel \forall n$. Then the class $-A$ contains the sequence $\{-q_n\}$ such that $-q_n > -\eta \parallel \forall n$, the number $-\eta$ is positive, then $-A$ is a positive class.

We also need to show that the set of positive classes is closed under addition and multiplication. Let A, B are any positive classes, then, as earlier, we take $\{q_n\} \in A \parallel q_n > \Delta > 0 \forall n$ and $\{p_n\} \in B \parallel p_n > \delta > 0 \forall n$. The class $A + B$ contains the sequence $\{q_n + p_n\} \parallel q_n + p_n > \Delta + \delta > 0$, so this class is positive. The class $A \cdot B$ contains the sequence $\{q_n \cdot p_n\} \parallel q_n \cdot p_n > \Delta \cdot \delta > 0$ and this class is also positive. Everything is proved.

Assertion3. The **Archimedes axiom** is true in R_{aux} .

Proof. Let's fix an arbitrary pair of **positive** classes A, B . We need to show that there exist some natural n such that $n \cdot A > B$. Notice, A^{-1} is positive, because $A \cdot A^{-1} = I$, where I is positive. If we assume that A^{-1} is negative, then $A \cdot A^{-1}$ must be negative (it is a basic property of ordered rings/fields, all these properties were listed earlier).

Let's multiply the equality $n \cdot A > B$ from the right side by A^{-1} , we will get $n \cdot I > B \cdot A^{-1}$. So, the equalities $n \cdot A > B$ and $n \cdot I > B \cdot A^{-1}$ are obviously equivalent (if we multiply both sides of the second one by A , we will get the first one). The class $B \cdot A^{-1}$ is positive. If we show that for any positive class P there exist some natural n such that $n \cdot I > P$, then everything will be proved. Let's fix an arbitrary positive class P and a positive sequence $\{p_m\} \in P \parallel p_m > \delta > 0$, this sequence is fundamental, therefore it is bounded, then there exist some rational $M > 0$ such that $|p_m| < M \forall m \Leftrightarrow p_m < M \forall m$. According to the [property5](#) of rational numbers, the rational number M lies between two integers $k \leq M < k + 1$. The integer number $k + 1$ is positive, then $k + 1$ is a natural number, let's take $n \equiv k + 1$, then we have $n > p_m > \delta > 0 \forall m$. Then $(n + 1) \cdot I > P$. Really, $(n + 1) \cdot I$ is the class which contains the sequence $(n + 1), (n + 1), (n + 1), \dots$ and P contains the sequence $\{p_m\} = p_1, p_2, p_3, \dots$. The class $(n + 1) \cdot I - P$ contains the sequence $((n + 1) - p_1), ((n + 1) - p_2), ((n + 1) - p_3), \dots$, all the terms of this sequence are greater than 1 (because $p_m < n \forall m$). So, the class $(n + 1) \cdot I - P$ is positive and $(n + 1) \cdot I > P$. Everything is proved.

For any rational number $q \in Q$, the stationary sequence $\{q\} \equiv q, q, q, q, q, \dots$ is fundamental, and therefore there exist the class $A \in R_{aux}$ which contains this sequence. For different rational numbers $p \neq q$ the stationary sequences $\{q\} \equiv q, q, q, q, q, \dots$ and $\{p\} \equiv p, p, p, p, p, \dots$ are not equivalent, therefore they belong to different classes $A, B \in R_{aux}$. A class $A \in R_{aux}$ may contain only one stationary sequence (because different stationary sequences are not equivalent). If A contains some stationary sequence, then we say “ A is a stationary class”.

Def. Every stationary class $A \in R_{aux}$, which contains some sequence $\{q\} \equiv q, q, q, q, q, \dots$, we replace by the rational number q . The set R_{aux} will turn into the set R which consists of rational numbers and classes of equivalent fundamental sequences: $R = Q \cup (\text{Classes of Sequences})$.

The set R is called a set of real numbers and elements of R are called real numbers.

Let's define addition and multiplication on R . At first we define the mapping: $f : R_{aux} \rightarrow R$.

For any stationary class $A \in R_{aux}$ which contains some $\{q\} \equiv q, q, q, q, q, \dots$ we define $f(A) \equiv q$, and for any other class $A \in R_{aux}$ we define $f(A) \equiv A$. Then f is one-to-one mapping $R_{aux} \rightarrow R$,

$$\begin{array}{ccc} & \text{(Stationary classes)} & \text{(Other classes)} \\ f : R_{aux} \rightarrow R \Leftrightarrow & \downarrow & \downarrow \\ & Q & \text{(Other classes)} \end{array} \quad . \text{ Any element } a \in R \text{ has the unique}$$

representation as an image of some class $A \in R_{aux} : a = f(A)$.

$$\begin{array}{l} \text{Then we define } \forall a, b \in R \Rightarrow \\ \begin{array}{l} a + b = f(A) + f(B) \equiv / \text{by definition} / \equiv f(A + B) \in R \\ a \cdot b = f(A) \cdot f(B) \equiv / \text{by definition} / \equiv f(A \cdot B) \in R \end{array} \end{array}$$

From the **theorem4** (page 40) immediately follows that $(R, +, \cdot)$ is a field.

From the **theorem5 (Transfer of order)** follows that R is an ordered field.

The field $(R, +, \cdot)$ is called a field of real numbers.

As the **Archimedes axiom** is true in R_{aux} , this axiom is true in R . Really, let's fix arbitrary positive $a, b \in R$. There exist the unique representations $a = f(A)$, $b = f(B)$. And the classes A, B are positive in R_{aux} (because f conserves the order):

$a > 0$ (in R) $\Leftrightarrow f(A) > f(O)$ (in R) $\Leftrightarrow A > O$ (in R_{aux}) $\Rightarrow A$ is positive (in R_{aux}). And B is also positive (in R_{aux}). As the **Archimedes axiom** is true in R_{aux} , there exist n such that $nA > B$, then $f(nA) > f(B) \Leftrightarrow f(A + A + A + \dots + A) > f(B) \Leftrightarrow f(A) + f(A) + f(A) + \dots + f(A) > f(B) \Leftrightarrow n \cdot f(A) > f(B) \Leftrightarrow n \cdot a > b$. So, the **Archimedes axiom** is true in R .

Assertion4. The addition and multiplication on R are extensions of the addition and multiplication on Q , i.e., for any $a, b \in Q \subset R$ we have:

$a + b$ (addition by the rules of R) = $a + b$ (addition by the rules of Q),

$a \cdot b$ (multiplication by the rules of R) = $a \cdot b$ (multiplication by the rules of Q).

And similarly, the order relation " $>$ " on R is an extension of the order relation on Q :

$a > b$ (by the rules of R) $\Leftrightarrow a > b$ (by the rules of Q).

Proof. Let's denote for a while $(\tilde{+}, \tilde{\cdot})$ - the addition and multiplication on the field R .

Let's fix arbitrary $a, b \in Q \subset R$. In order to find their sum/product we need to find their representations as images of some classes $A, B \in R_{aux}$, so $a = f(A)$ and $b = f(B)$. As $a, b \in Q$, the classes A, B are stationary classes, the class A contains the sequence $\{a\} = a, a, a \dots$ and B contains the sequence $\{b\} = b, b, b \dots$. By definition $a \tilde{+} b = f(A) \tilde{+} f(B) = /by def/ = f(A + B)$. The class $A + B$ contains the sequence $\{a\} + \{b\} = a + b, a + b, a + b \dots$, therefore $A + B$ is a stationary class, then $f(A + B) = a + b$, then $a \tilde{+} b = a + b$.

Next, $a \tilde{\cdot} b = f(A) \tilde{\cdot} f(B) = /by def/ = f(A \cdot B)$. The class $A \cdot B$ contains the sequence $\{a\} \cdot \{b\} = a \cdot b, a \cdot b, a \cdot b \dots$, therefore $A \cdot B$ is a stationary class, then $f(A \cdot B) = a \cdot b$, then $a \tilde{\cdot} b = a \cdot b$. Next, let $a > b \Leftrightarrow f(A) > f(B)$ (in R), as f conserves the order, then $A > B$ (in R_{aux}), then $A - B = A + (-B)$ is a positive class in R_{aux} , this class contains the sequence $\{a\} + \{-b\} = a - b, a - b, a - b \dots$. So, the sequence $a - b, a - b, a - b \dots$ belongs to the positive class $A - B$. According to [auxiliary1](#), the positive class $A - B$ contains some sequence $\{q_n\} \parallel q_n > \rho > 0 \forall n$. If $a - b \leq 0$, then every term of the sequence $\{q_n - (a - b)\}$ is greater than $\rho > 0$, so this sequence can't be infinitely small. But $\{q_n - (a - b)\}$ must be infinitely small, because the sequences $\{q_n\}$ and $\{a - b\}$ belong to the same class. **Then** $a - b > 0 \Rightarrow a > b$.

We have deduced that from $a > b$ (in R) follows that $a > b$ (in Q).

Conversely: $a > b$ (in Q). Let's consider the stationary class $A \in R_{aux}$ which contains the sequence $\{a\} = a, a, a \dots$ and the class $B \in R_{aux}$ which contains the sequence $\{b\} = b, b, b \dots$.

The class $A - B = A + (-B)$ contains the sequence $a - b, a - b, a - b \dots$, every term of this sequence is greater than the positive number $(a - b)/2$, then $A - B$ is a positive class, then $A > B$ (in R_{aux}), then (conservation of order) $f(A) > f(B)$ (in R) $\Leftrightarrow a > b$ (in R). Everything is proved

Consequence2. Now we can say: R is an ordered field which contains the field of rational numbers Q as a subfield. From here follows that all the results that we got earlier in the chapter "Sequences and limits" can be applied to R . As the **Archimedes axiom** is true in R ([assertion3](#)), then, according to the [theorem1](#):

[A] Any sequence $\{q_n\} \subset Q$ which converges/fundamental in Q also converges/fundamental in R

[B] Any element $a \in R$ can be represented as a limit of some rational sequence $\{q_n\} \subset Q$.

Theorem2. An element $a \in R$ is an image of a class $A \in R_{aux}$ (so $a = f(A)$).

Let $\{q_n\} = q_1, q_2, q_3, q_4 \dots$ is any fundamental sequence from A . Then the sequence of rational numbers $\{q_n\} = q_1, q_2, q_3, q_4 \dots \subset Q \subset R$ converges to a in the field R .

Auxiliary3. Let $A \in R_{aux}$ and $\{q_n\} = q_1, q_2, q_3, q_4 \dots$ is any fundamental sequence from A .

Let's consider the sequence of stationary classes $St(q_1), St(q_2), \dots, St(q_n), \dots$ of R_{aux} . Where $St(q_1)$ is a stationary class with the sequence $q_1, q_1, q_1 \dots$ and $St(q_2)$ is a stationary class with the sequence $q_2, q_2, q_2 \dots$ and etc. Let's show that for any positive class $\Sigma \in R_{aux}$ there exist \bar{k} , such that $\forall \bar{n} > \bar{k}$ we have $|A - St(q_{\bar{n}})| < \Sigma$.

(Notice, here we would like to say that A is a limit of stationary classes $St(q_1), St(q_2), \dots, St(q_n), \dots$, but we have defined what is a limit of a sequence for sequences of any ordered field which contains the field of rational numbers, and in our case elements of R_{aux} are the classes of equivalent sequences, so there are no any rational numbers in R_{aux} . And we can't use the limit-notion in R_{aux} .

[Step1] Let's show that for any positive stationary class $P \in R_{aux}$ there exist the natural number \bar{k} such that $\forall n > \bar{k}$ we have $|A - St(q_n)| < P$. Let's fix any positive stationary class $P \in R_{aux}$, it contains some sequence $p, p, p, \dots \parallel p > 0$. The sequence $\{q_n\} \in A$ is fundamental, then for $p/2 > 0$ there exist the natural number \bar{k} , such that $\forall n, \bar{n} > \bar{k}$ we have $|q_n - q_{\bar{n}}| < p/2$ [L]. We fix now the numbers \bar{k}, \bar{n} , where \bar{n} is an **arbitrary natural** number $\bar{n} > \bar{k}$.

The class $A - St(q_{\bar{n}})$ contains the sequence $\{q_n - q_{\bar{n}}\}$. The absolute value of every term of the sequence $\{q_n - q_{\bar{n}}\}$ with number $n > \bar{k}$ is less than $p/2$ [L]. It may not be true for the terms with numbers $m < \bar{k}$, let's then replace every term with number $m < \bar{k}$ by a constant $p/4$.

Then we have the new sequence, and now the absolute value of every term is less than $p/2$, and the new sequence belongs to the same class $A - St(q_{\bar{n}})$ (because it is equivalent to the initial one). So we have $\{v_n\} \in A - St(q_{\bar{n}})$ such that $|v_n| < p/2 \forall n$.

Let's consider now the class P with the sequence p, p, p, \dots . Let's show that $|A - St(q_{\bar{n}})| < P$, this inequality is equivalent to $-P < A - St(q_{\bar{n}}) < P$. Let's show at first that $A - St(q_{\bar{n}}) < P$. Really, the class $P - (A - St(q_{\bar{n}}))$ contains the sequence $\{p\} - \{v_n\} = \{p - v_n\}$ and we know that $|v_n| < p/2 \forall n \Leftrightarrow -p/2 < v_n < p/2$, then $p - v_n > p - p/2 > p/2$ so, every term of the sequence $\{p - v_n\}$ is greater than the positive number $p/2$, then the class $P - (A - St(q_{\bar{n}}))$ (which contains this sequence) is positive (by definition). Then $A - St(q_{\bar{n}}) < P$.

Let's show now that $-P < A - St(q_{\bar{n}})$. The class $(A - St(q_{\bar{n}})) - (-P)$ contains the sequence

$\{v_n\} - \{-p\} = \{v_n + p\}$ and again, from the condition $|v_n| < p/2 \quad \forall n \Leftrightarrow -p/2 < v_n < p/2$ we have $v_n + p > -p/2 + p = p/2$ so, every term of the sequence $\{v_n + p\}$ is greater than $p/2 > 0$.

Then the class $(A - St(q_{\bar{n}})) - (-P)$ is positive, then $-P < A - St(q_{\bar{n}})$.

So, for any positive stationary class P there exist \bar{k} , such that for any $\bar{n} > \bar{k}$ we have $|A - St(q_{\bar{n}})| < P$.

[Step2] Let's fix an arbitrary positive class $\Sigma \in R_{aux}$ there exist some sequence

$\{\varepsilon_n\} \in \Sigma \parallel \varepsilon_n > \rho > 0 \quad \forall n$. Let's consider the positive stationary class P which contains the sequence $\rho/2, \rho/2, \rho/2, \dots$. The class $\Sigma - P$ is positive, really, it contains the sequence $\{\varepsilon_n - \rho/2\}$, and all the terms of this sequence are greater than the positive number $\rho/2$. Then $\Sigma > P$. For the class P there exist \bar{k} , such that for any $\bar{n} > \bar{k}$ we have $|A - St(q_{\bar{n}})| < P$, then $|A - St(q_{\bar{n}})| < P < \Sigma$.

So, for any positive class $\Sigma \in R_{aux}$ there exist \bar{k} , such that for any $\bar{n} > \bar{k}$ we have $|A - St(q_{\bar{n}})| < \Sigma$.

Let's prove now the **theorem3**. We fix an arbitrary element $a \in R$ and the unique $A \in R_{aux}$ such that $a = f(A)$. Let's take an arbitrary $\{q_n\} \in A$, we want to show that $\{q_n\} \rightarrow a$ in the field R .

Let's fix an arbitrary positive element $\varepsilon \in R$. The mapping $f : R_{aux} \rightarrow R$ conserves the order, if $\varepsilon = f(\Sigma)$, then Σ is positive in R_{aux} , really, $\varepsilon > 0$ (in R) $\Leftrightarrow f(\Sigma) > f(0)$ (in R) $\Leftrightarrow \Sigma > 0$ (in R_{aux}).

For the positive class Σ there exist \bar{k} such that for any $\bar{n} > \bar{k}$ we have

$$|A - St(q_{\bar{n}})| < \Sigma \Leftrightarrow -\Sigma < A - St(q_{\bar{n}}) < \Sigma \Rightarrow / f \text{ conseves the order} / \Rightarrow f(-\Sigma) < f(A - St(q_{\bar{n}})) < f(\Sigma)$$

Remember the basic properties of any ring/field isomorphism: $f(-a) = -f(a)$ and

$f(a - b) = f(a) - f(b)$. Then we can rewrite $-f(\Sigma) < f(A) - f(St(q_{\bar{n}})) < f(\Sigma)$. The image of the class A is the element a , the image of $St(q_{\bar{n}})$ is the rational number $q_{\bar{n}}$, so we can rewrite $-\varepsilon < a - q_{\bar{n}} < \varepsilon \Rightarrow |a - q_{\bar{n}}| < \varepsilon$. We have deduced that: for any positive $\varepsilon \in R$ there exist \bar{k} , such that for any $\bar{n} > \bar{k}$ we have $|a - q_{\bar{n}}| < \varepsilon$. It means exactly that $\{q_n\} \rightarrow a$.

Theorem3. R is a complete field.

Proof. We will use the **consequence2** and the **theorem2**. Let's fix an arbitrary fundamental sequence $\{a_k\} \subset R$. Our goal is to show that it converges to some $a \in R$. According to the **consequence2** [B], every element a_k can be represented as a limit of some rational sequence $q_1^k, q_2^k, q_3^k, \dots = \{q_n^k\} \rightarrow a_k$. Let's fix now an infinitely small rational sequence $\{1/k\} \rightarrow 0$. This sequence is infinitely small in Q , and, according to the **consequence2** [A], it is infinitely small in R . For every a_k we can find and fix one element from $\{q_n^k\} \rightarrow a$ (let's denote it q_k^k) such that $|a_k - q_k^k| < 1/k$.

So, we have the sequence $q_1^1, q_2^2, q_3^3, \dots \equiv \{q_k^k\}$ such that $|a_k - q_k^k| < 1/k$ for any k .

The sequence $\{q_k^k\}$ is a rational sequence. From the conditions: $\{a_k\}$ is fundamental and $|a_k - q_k^k| < 1/k \forall k$ follows that $\{q_k^k\}$ is also fundamental. Really, let's take the condition $|a_k - q_k^k| < 1/k \Leftrightarrow -1/k < a_k - q_k^k < 1/k$. We can denote $\alpha_k \equiv a_k - q_k^k$, then $-1/k < \alpha_k < 1/k$, according to the squeeze theorem for sequences, $\{\alpha_k\}$ is infinitely small in R , then $\{\alpha_k\}$ is fundamental in R . According to the [consequence9](#), the difference of fundamental sequences is a fundamental sequence. And we have $\alpha_k = a_k - q_k^k \Leftrightarrow q_k^k = a_k - \alpha_k \Leftrightarrow \{q_k^k\} = \{a_k\} - \{\alpha_k\}$, then $\{q_k^k\}$ is a fundamental sequence of rational numbers. Then there exist the class $A \in R_{aux}$ which contains the sequence $\{q_k^k\}$. According to the [theorem2](#), the image $a = f(A) \in R$ is a limit of the rational sequence $\{q_k^k\} \subset R$. Then the fundamental sequence $\{q_k^k\}$ actually goes to $a \in R$. Then the initial sequence $\{a_k\}$ goes to the same limit a . Really, we have $\alpha_k \equiv a_k - q_k^k \Leftrightarrow \{\alpha_k\} \equiv \{a_k\} - \{q_k^k\}$, so the sequence $\{a_k\} - \{q_k^k\}$ is infinitely small and $\{q_k^k\} \rightarrow a$. Then, according to the [consequence6](#), we have $\{a_k\} \rightarrow a$. So, the fundamental sequence $\{a_k\} \subset R$ converges to $a \in R$. Everything is proved.

Assertion5. For any real number $a \in R$ there exist the unique pair of integer numbers $k, k+1$ such that $k \leq a < k+1$. The proof is exactly the same as the proof of the similar assertion ([property5](#)) for rational numbers.

Uniqueness of real numbers.

Def. $\{x_n\}$ converges, then it's limit can be denoted as $\lim x_n$ or $\lim_{n \rightarrow \infty} x_n$.

All fields of rational numbers are isomorphic. But formally, there exist different fields of rational numbers, and based on these fields we can construct formally different fields of real numbers. Let's show that all these fields are also isomorphic.

Uniqueness theorem. Any fields R_A and R_B of real numbers are isomorphic. Moreover, the isomorphism $f: R_A \rightarrow R_B$ is unique, this isomorphism is an extension of the unique isomorphism $f: Q_A \rightarrow Q_B$ where $Q_A \subset R_A$, $Q_B \subset R_B$.

Proof. Existence. Let's extend the unique isomorphism $f: Q_A \rightarrow Q_B$ up to $f: R_A \rightarrow R_B$.

We define: for any $a_A \in R_A$ if $\{q_n\} \rightarrow a_A$ (in R_A) $\parallel \{q_n\} \subset Q_A$, then

$f(a_A) \equiv /by def/ \equiv \lim f(q_n)$ (in R_B). As we know, every element $a_A \in R_A$ can be represented as a limit of some rational sequence $\{q_n\} \subset Q_A$. Let's outline the main steps of our proof. In [\[A\]](#) we will show that if $\{q_n\} \subset Q_A$ converges in R_A , then $\{f(q_n)\}$ converges in R_B . From here follows that for any $a_A \in R_A$ the element(s) $f(a_A) \in R_B$ is defined.

In [B] we will show that for any $a_A \in R_A$ the element $f(a_A)$ is uniquely defined, i.e., for any sequence $\{q_n\} \rightarrow a_A$ the limit $\lim f(q_n)$ is always the same. After [A] and [B] we are able to say that: f is a mapping from R_A to R_B .

In [C] we will show that f coincides with the unique isomorphism $f: Q_A \rightarrow Q_B$ on the set Q_A . Then the new f is really an extension of the old f .

In [D] we will show that $f: R_A \rightarrow R_B$ is one-to-one mapping. And finally in [E] we will show that f has the basic properties of any isomorphism: $\forall a_A, b_A \in R_A \parallel f(a_A + b_A) = f(a_A) + f(b_A)$ and $f(a_A \cdot b_A) = f(a_A) \cdot f(b_A)$.

Let's start. [A] Let $\{q_n\} \rightarrow a_A$ (in R_A) $\parallel \{q_n\} \subset Q_A$, then $\{q_n\}$ is fundamental in R_A , then $\{q_n\}$ is fundamental in $Q_A \subset R_A$. Let's show that $\{f(q_n)\}$ is fundamental in Q_B . Let's fix an arbitrary positive $\varepsilon_B \in Q_B$, there exist the unique positive $\varepsilon_A \in Q_A$ such that $f(\varepsilon_A) = \varepsilon_B$.

As $\{q_n\}$ is fundamental in Q_A , there exist

$$\begin{aligned} k \in \mathbb{N} : \forall m, n > k \Rightarrow |x_m - x_n| < \varepsilon_A &\Leftrightarrow -\varepsilon_A < x_m - x_n < \varepsilon_A \Rightarrow / f: Q_A \rightarrow Q_B \text{ conserves } "<"/ \Rightarrow \\ \Rightarrow f(-\varepsilon_A) < f(x_m - x_n) < f(\varepsilon_A) &\Leftrightarrow -f(\varepsilon_A) < f(x_m) - f(x_n) < f(\varepsilon_A) \Leftrightarrow -\varepsilon_B < f(x_m) - f(x_n) < \varepsilon_B \\ \Leftrightarrow |f(x_m) - f(x_n)| < \varepsilon_B. &\text{ So, for any positive } \varepsilon_B \in Q_B \text{ there exist} \end{aligned}$$

$$k \in \mathbb{N} : \forall m, n > k \Rightarrow |f(x_m) - f(x_n)| < \varepsilon_B \text{ and therefore } \{f(q_n)\} \text{ is fundamental in } Q_B.$$

As the **Archimedes axiom** is true in R_B (**theorem1**), the sequence $\{f(q_n)\}$ is fundamental in R_B .

As R_B is a complete field, the sequence $\{f(q_n)\}$ converges to some element of R_B .

So, the limit $\lim f(q_n) \equiv f(a_A)$ exists.

[A1] (During the proof of [A] we have shown that $f: Q_A \rightarrow Q_B$ transfers any fundamental rational sequence into a fundamental rational sequence)

[B] Let $\{q_n\} \rightarrow a_A$ and $\{p_n\} \rightarrow a_A$, then $\{q_n - p_n\}$ is infinitely small in R_A , then $\{q_n - p_n\}$ is infinitely small in Q_A . Let's show that $\{f(q_n - p_n)\} = \{f(q_n) - f(p_n)\}$ is infinitely small in Q_B .

Let's fix any positive $\varepsilon_B \in Q_B$, there exist the unique $\varepsilon_A \in Q_A$ such that $f(\varepsilon_A) = \varepsilon_B$.

$$\begin{aligned} \text{As } \{q_n - p_n\} \text{ is infinitely small in } Q_A, \text{ for } \varepsilon_A \text{ there exist } k \in \mathbb{N} : \forall n > k \Rightarrow |q_n - p_n| < \varepsilon_A &\Leftrightarrow \\ -\varepsilon_A < q_n - p_n < \varepsilon_A \Rightarrow f(-\varepsilon_A) < f(q_n - p_n) < f(\varepsilon_A) &\Leftrightarrow -f(\varepsilon_A) < f(q_n) - f(p_n) < f(\varepsilon_A) \Leftrightarrow \\ -\varepsilon_B < f(q_n) - f(p_n) < \varepsilon_B &\Leftrightarrow |f(q_n) - f(p_n)| < \varepsilon_B, \text{ then } \{f(q_n) - f(p_n)\} \text{ is infinitely small in } Q_B. \end{aligned}$$

Then (**theorem1**) $\{f(q_n) - f(p_n)\}$ is infinitely small in R_B . We already know that $\{f(q_n)\}$ converges to some limit in R_B , then (**consequence6**) $\{f(p_n)\}$ converges to the same limit in R_B .

[B1] (During the proof of [B] we have shown that $f: Q_A \rightarrow Q_B$ transfers any infinitely small rational sequence into an infinitely small rational sequence).

[C] Let's fix an arbitrary $q_A \in Q_A$ then q_A is a limit of the stationary sequence q_A, q_A, q_A, \dots

According to the new definition, the image of q_A is defined as a limit of the sequence $f(q_A), f(q_A), f(q_A), \dots$, it is a stationary sequence of Q_B , and it obviously converges to $f(q_A) \in Q_B$. So, the new mapping is really an extension of the old one.

[D] [Step1] f fully covers the set R_B . Let's fix any element $a_B \in R_B$, it can be represented as a limit $\{q_n^B\} \rightarrow a_B$. Every element $q_n^B \in Q_B$ has the unique representation $q_n^B = f(q_n^A) \parallel q_n^A \in Q_A$. As $\{q_n^B\}$ converges in R_B , then $\{q_n^B\}$ is fundamental in R_B .

Remember that $f: Q_A \rightarrow Q_B$ is a field isomorphism, then $f^{-1}: Q_B \rightarrow Q_A$ is also a field isomorphism, we have shown above (**[A1]**) that such isomorphism transfers any fundamental rational sequence into a fundamental rational sequence, so f^{-1} transfers $\{q_n^B\}$ which is fundamental in R_B , into $\{q_n^A\}$ which is fundamental in R_A . Then $\{q_n^A\}$ converges in R_A to some element $a_A \in R_A$. And we have: $\{q_n^A\} \rightarrow a_A$ (in R_A) and also $\{f(q_n^A)\} = \{q_n^B\} \rightarrow a_B \in R_B$, so $f(a_A) = a_B$ and any element $a_B \in R_B$ has at least one preimage in R_A .

[Step2] f doesn't glue together elements of R_A . Let's assume that $a_A \neq b_A$ and $f(a_A) = f(b_A)$.

Let $\{q_n\} \rightarrow a_A$ and $\{p_n\} \rightarrow b_A$. As $f(a_A) = f(b_A)$, then $\lim f(q_n) = \lim f(p_n)$, then the sequence $\{f(q_n) - f(p_n)\}$ is infinitely small in R_B . According to **[B1]**, $f^{-1}: Q_B \rightarrow Q_A$ transfers any infinitely small rational sequence into an infinitely small rational sequence. So $f^{-1}: Q_B \rightarrow Q_A$ transfers $\{f(q_n) - f(p_n)\} \subset Q_B$ into $\{f^{-1}(f(q_n) - f(p_n))\} = \{f^{-1}(f(q_n)) - f^{-1}(f(p_n))\} = \{q_n - p_n\}$ -this sequence is infinitely small in R_A . Then both sequences $\{q_n\}$ and $\{p_n\}$ converge to the same limit in R_A and $a_A = b_A$, and we have a contradiction. So, if $a_A \neq b_A$ there must be $f(a_A) \neq f(b_A)$. From the **[Step1]** and **[Step2]** follows that $f: R_A \rightarrow R_B$ is one-to-one.

[E] Let's fix arbitrary elements $\forall a_A, b_A \in R_A$, and let's fix any sequences $\{q_n\}, \{p_n\} \subset Q_A$ such that $\{q_n\} \rightarrow a_A$ and $\{p_n\} \rightarrow b_A$ in R_A . Let's find $f(a_A) + f(b_A)$. As $f(a_A) = \lim f(q_n)$ and $f(b_A) = \lim f(p_n)$, then $f(a_A) + f(b_A) = \lim f(q_n) + \lim f(p_n) = \lim(f(q_n) + f(p_n)) = \lim(f(q_n + p_n))$ **[Y]**- we have here the limit of the sequence $\{f(q_n + p_n)\}$.

As $\{q_n\} \rightarrow a_A$ and $\{p_n\} \rightarrow b_A$, then $\{q_n + p_n\} \rightarrow a_A + b_A$. Then, by definition of f , we have $f(a_A + b_A) = \lim(f(q_n + p_n))$ - let's compare this result with **[Y]**, then $f(a_A) + f(b_A) = f(a_A + b_A)$.

Next. Let's find $f(a_A) \cdot f(b_A)$. As $f(a_A) = \lim f(q_n)$ and $f(b_A) = \lim f(p_n)$, then

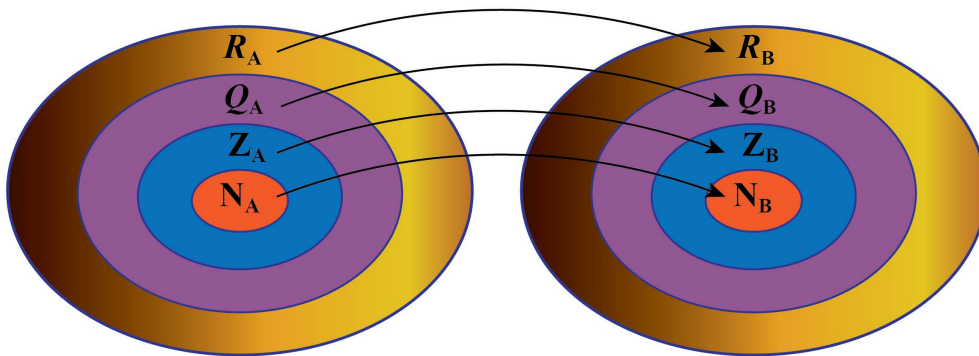
$$f(a_A) \cdot f(b_A) = \lim f(q_n) \cdot \lim f(p_n) = \lim(f(q_n) \cdot f(p_n)) = \lim(f(q_n \cdot p_n)) \text{ [U].}$$

As $\{q_n\} \rightarrow a_A$ and $\{p_n\} \rightarrow b_A$, then $\{q_n \cdot p_n\} \rightarrow a_A \cdot b_A$. Then, by definition of f , we have $f(a_A \cdot b_A) = \lim q_n \cdot p_n$ - let's compare this result with **[U]**, then $f(a_A) \cdot f(b_A) = f(a_A \cdot b_A)$.

Uniqueness. Let we have some isomorphism $\varphi: R_A \rightarrow R_B$, as φ is a field isomorphism, it transfers one into one and zero into zero: $\varphi(0_A) = 0_B$, $\varphi(1_A) = 1_B$ we can show (in exactly the same way as we did in the **uniqueness theorem** for rational numbers) that φ is an isomorphism $Z_A \rightarrow Z_B$ (where $Z_A \subset R_A, Z_B \subset R_B$) (it follows from the basic properties of isomorphism and conditions $\varphi(0_A) = 0_B$, $\varphi(1_A) = 1_B$). And then we can show that φ is an isomorphism $Q_A \rightarrow Q_B$ (the proof is exactly the same as a proof for rational numbers).

So $\varphi: Q_A \rightarrow Q_B \parallel Q_A \subset R_A, Q_B \subset R_B$ is an isomorphism. But there exist only one isomorphism $f: Q_A \rightarrow Q_B$, then $\varphi \equiv f$ on Q_A . Let's fix any element $a_A \in R_A$, there exist $\{q_n\} \subset Q_A \parallel \{q_n\} \rightarrow a_A$, then $f(a_A) = \lim f(q_n)$. Every element q_n belongs to Q_A , then $f(q_n) = \varphi(q_n)$, then the sequences $\{f(q_n)\}$ and $\{\varphi(q_n)\}$ are completely the same, then they have the same limit: $f(a_A) = \lim \varphi(q_n) = \lim f(q_n)$ [J]. From the condition $\{q_n\} \rightarrow a_A$ follows that $\{\varphi(q_n)\} \rightarrow \varphi(a_A)$ (show it, by using that $\varphi: R_A \rightarrow R_B$ is an isomorphism, remember that φ conserves the order " $>$ ", it follows from the **theorem** "Transfer of order"). So we have $\{\varphi(q_n)\} \rightarrow \varphi(a_A)$ and $\{\varphi(q_n)\} \rightarrow f(a_A)$, then $f(a_A) = \varphi(a_A)$, then $\varphi \equiv f$ on R_A .

Consequence. For any fields of real numbers R_A, R_B there exist the unique isomorphism $f: R_A \rightarrow R_B$ [pict1] which is an extension of the unique isomorphism $f: Q_A \rightarrow Q_B$ (where $Q_A \subset R_A, Q_B \subset R_B$) which is an extension of the unique isomorphism $f: Z_A \rightarrow Z_B$ (where $Z_A \subset Q_A \subset R_A, Z_B \subset Q_B \subset R_B$) which, in it's turn, is an extension of the unique isomorphism $f: N_A \rightarrow N_B$ (where $N_A \subset Z_A \subset Q_A \subset R_A, N_B \subset Z_B \subset Q_B \subset R_B$).



pict.1

Main properties of real numbers

Def. $a < b$ - are any real numbers. The set $\{x\}$ of real numbers such that $a \leq x \leq b$ is called a segment of real numbers, and we denote it $[a, b]$. The set $\{x\}$ of real numbers such that $a < x < b$ is called “an interval of real numbers”, and we denote it (a, b) . Similarly:
 $\{x \mid a \leq x < b\} \equiv / \text{by definition} / \equiv [a, b)$ and $\{x \mid a < x \leq b\} \equiv / \text{by definition} / \equiv (a, b]$ - half-intervals of real numbers.

Note. At this moment segments and intervals are just some sets in the field R , there can't be any representation of these segments/intervals like some sets on the line, because we haven't built one-to-one correspondence between the field R and some line L .
 In order to do it we need to define the “length”, and it will be done in the next chapter.
 Let's explore now the most important properties of real numbers.

Def. A sequence $\{a_n\}$ of real numbers is called monotonically increasing (or just increasing) if $a_n \leq a_{n+1} \forall n$ and monotonically decreasing (or just decreasing) if $a_n \geq a_{n+1} \forall n$.
 A sequence $\{a_n\}$ is called strictly increasing if $a_n < a_{n+1} \forall n$ and strictly decreasing if $a_n > a_{n+1} \forall n$.

Auxiliary1. If $\{a_n\} \rightarrow A$ and the sequence $\{a_n\}$ is monotonically increasing (in particular, strictly increasing), then $a_n \leq A \forall n$. If $\{b_n\} \rightarrow B$ and $\{b_n\}$ is monotonically decreasing (in particular strictly decreasing), then $B \leq b_n \forall n$.

Solution. $\{a_n\}$ is monotonically increasing. Let's assume that there exist some concrete number \bar{k} such that $A < a_{\bar{k}}$. As $\{a_n\}$ is monotonically increasing, then $a_{\bar{k}} \leq a_{\bar{k}+1} \leq a_{\bar{k}+2} \leq a_{\bar{k}+3} \leq \dots$
 Let's consider the neighborhood $O_\varepsilon(A)$ with the radius $\varepsilon = |A - a_{\bar{k}}|/2$. This neighborhood $O_\varepsilon(A)$ does not contain the term $a_{\bar{k}}$ and therefore it does not contain the next terms
 $a_{\bar{k}+1} < a_{\bar{k}+2} < a_{\bar{k}+3} < \dots$ (really, $\forall n \geq \bar{k} \Rightarrow |A - a_n| = a_n - A \geq a_{\bar{k}} - A = |a_{\bar{k}} - A| = |A - a_{\bar{k}}| > |A - a_{\bar{k}}|/2$,
 then $|A - a_n| > \varepsilon \Rightarrow a_n \notin O_\varepsilon(A)$). Therefore, A is not a limit of the sequence $\{a_n\}$,
 (because any neighborhood of A must contain all the terms, starting from some number, which is not true in our case), we have a contradiction. Then the number \bar{k} such that $A < a_{\bar{k}}$, doesn't exist.
 Then $a_n \leq A \forall n$. The proof is similar when $\{b_n\}$ is monotonically decreasing.

The Nested Segment Theorem. For any sequence of segments $[a_1, b_1] \supset [a_2, b_2] \supset [a_3, b_3] \supset \dots$ of real numbers such that $\{b_n - a_n\} \rightarrow 0$, there exist exactly one real number A which belongs to every segment $[a_n, b_n]$.

Proof. Let's consider the sequence of right ends $\{b_n\}$ and the sequence of left ends $\{a_n\}$.
 From $\{b_n - a_n\} \rightarrow 0$ follows that both sequences $\{a_n\}$ and $\{b_n\}$ are fundamental. Really, let's fix

an arbitrary $\varepsilon > 0$, and we can find the number k such that $\forall n > k : b_n - a_n < \varepsilon$.

Let's fix any pair of numbers $m, n > k$ and let's show that $|a_m - a_n| < \varepsilon$ and $|b_m - b_n| < \varepsilon$.

If $m = n$, then $|a_m - a_n| = 0$ and $|b_m - b_n| = 0$.

If $m > n$, then $|a_m - a_n| = a_m - a_n < [as\ a_m < b_n] < b_n - a_n < \varepsilon$.

And $|b_m - b_n| = b_n - b_m < [as\ a_n < b_m] < b_n - a_n < \varepsilon$. There is no need to consider the case $n > m$, because $|a_m - a_n| = |a_n - a_m|$ and $|b_m - b_n| = |b_n - b_m|$.

Then for any $\varepsilon > 0$ there exist k , such that $\forall m, n > k$ we have $|a_m - a_n| < \varepsilon$ and $|b_m - b_n| < \varepsilon$, then both sequences $\{a_n\}$ and $\{b_n\}$ are fundamental. As R is a complete field, both these sequences must converge: $\{a_n\} \rightarrow A$ and $\{b_n\} \rightarrow B$. Let's denote $\alpha_n \equiv b_n - a_n$, from the condition $\{b_n - a_n\} \rightarrow 0$ follows that $\{\alpha_n\}$ is an infinitely small sequence. Then ([consequence5 in sequences and limits](#)) we have $A = B$. So, both sequences converge to the same limit: $\{a_n\} \rightarrow A$ and $\{b_n\} \rightarrow A$. The sequence $\{a_n\}$ is monotonically increasing, then ([auxiliary1](#) above) we have $a_n \leq A \ \forall n$, the sequence $\{b_n\}$ is monotonically decreasing, then ([auxiliary1](#) above) $A \leq b_n \ \forall n$. So $a_n \leq A \leq b_n \ \forall n$ it means that A belongs to every segment $[a_n, b_n]$.

Uniqueness. Let's assume that there exist some other number $B \in [a_n, b_n] \ \forall n$, where $B \neq A$. Without loss of generality $B < A$. So, we have $a_n \leq B \leq b_n \ \forall n$ and $a_n \leq A \leq b_n \ \forall n$ and $a_n \leq B < A \leq b_n \ \forall n$, then every difference $b_n - a_n$ is greater than the fixed positive number $(A - B) > 0$, then there can't be $\{b_n - a_n\} \rightarrow 0$ and we have a contradiction. Everything is proved.

Def1. A set X of real numbers is called bounded above if there exist some number \tilde{M} such that $\forall x \in X : x \leq \tilde{M}$. The number \tilde{M} in such case is called an upper bound of the set X .

An upper bound \tilde{M} is not unique. If \tilde{M} is an upper bound of X , then any $\tilde{\tilde{M}} > \tilde{M}$ is also an upper bound of M .

Def2. The number M is called “the least upper bound of X ”, or just a “supremum of X ”, if [1] M is an upper bound of X [2] for any other upper bound $\tilde{M} \neq M$ of X we have $M < \tilde{M}$.

Example. The number 1 is the least upper bound for the next sets: $[0,1)$, $[-2,1]$, $[1,1]$, $\{1 - 1/n \mid n \in \mathbb{N}\}$.

Exercise. From the [def2](#) immediately follows that: if X has the least upper bound M , then M is unique.

Upper bound criterion. M is the least upper bound of $X \Leftrightarrow M$ is greater than any element of X and for any positive number $\varepsilon > 0$ the set $(M - \varepsilon, M]$ contains at least one element of X .

Proof. \Rightarrow Let M is the least upper bound of X . The requirement “ M is greater than any element of X ” is automatically true. Let there exist some $\varepsilon > 0$ such that $(M - \varepsilon, M]$ does not contain any elements of X . Then any number from the interval $(M - \varepsilon, M)$ is greater than any element of X and less than M , so M is not the least upper bound. We got a contradiction. Then $\forall \varepsilon > 0$ the interval $(M - \varepsilon, M]$ contains at least one element of M .

Conversely. \Leftarrow From the requirement “ M is greater than any element of X ” follows that M is an upper bound of X . Let's assume that there exist some other upper bound $\tilde{M} \neq M$ of X such that $\tilde{M} < M$, then the half-interval $(\tilde{M}, M]$ (it is an interval $(M - \varepsilon, M]$ in the case $\varepsilon = M - \tilde{M}$) does not contain any elements of X . And we have a contradiction. So, if $\tilde{M} \neq M$, then there must be $M < \tilde{M}$ and M is the least upper bound (def2).

The next theorem is one of the most important in math and there will be a very simple proof of it.

Least upper bound property. Any non-empty set X of real numbers, which is bounded above, has the least upper bound M .

Proof. Let's fix an arbitrary set X and any upper bound \tilde{M} of X . Let's also fix some number T which is less than some (any one) element of X . Then the segment $[T, \tilde{M}]$.

[1] Contains at least one element of the set X .

[2] The “right end” of this segment (now it is \tilde{M}) is greater than any element of X .

Let's divide $[T, \tilde{M}]$ into two segments $\left[T, \frac{T + \tilde{M}}{2}\right] \equiv [a_1, b_1]$ and $\left[\frac{T + \tilde{M}}{2}, \tilde{M}\right] \equiv [b_1, c_1]$.

It's easy to check that exactly one of these segments ($[a_1, b_1]$ or $[b_1, c_1]$) also satisfies to the conditions [1] and [2] [pic2].

Without loss of generality, let now $[a_1, b_1]$ satisfies to [1] and [2]. Then we divide

$[a_1, b_1]$ into two segments $\left[a_1, \frac{a_1 + b_1}{2}\right]$

and $\left[\frac{a_1 + b_1}{2}, b_1\right]$. And again, exactly one

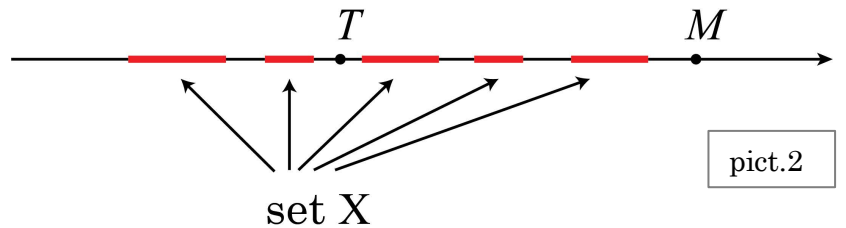
of these two segments must satisfy to [1]

and [2], we denote this segments as $[a_2, b_2]$, and we continue the process. As a result we have

the sequence $\{[a_n, b_n]\}$ of nested segments, it's easy to see that for any $n \geq 1$ we have

$b_n - a_n = (b_{n-1} - a_{n-1})/2$ and therefore, for any $n \geq 2$ we have $b_n - a_n = (b_1 - a_1)/2^{n-1}$, then

obviously $\{b_n - a_n\} \rightarrow 0$ and (according to the **nested segment theorem**, that is proved above)



pict.2

Comment: we haven't built yet one-to-one correspondence between real numbers and points on the line. Anyway, this picture can be used for convenience.

there exist the unique number M which belongs to every segment $[a_n, b_n]$. Let's show that M satisfies to the upper bound criterion (and therefore, M is the least upper bound of X).

[A] M is greater than any element of X . Really, let's assume that there exist $\tilde{x} \in X$ such that $\tilde{x} > M$. Let's consider the interval (M, \tilde{x}) . Starting from some number k all the "right ends" b_n of the segments $[a_n, b_n]$ belong the interval (M, \tilde{x}) . Really, we have $a_n \leq M \leq b_n$, if $b_n \notin (M, \tilde{x})$, then $b_n > \tilde{x}$ and therefore $b_n - a_n > \tilde{x} - a_n \geq [as\ a_n \leq M] \geq \tilde{x} - M = const > 0$, so $b_n - a_n > const$, it can't be true for every n , because $\{b_n - a_n\} \rightarrow 0$. Then there exist k such that $b_k \in (M, \tilde{x})$, then all the next right ends $b_{k+1}, b_{k+2}, b_{k+3}, \dots \in (M, \tilde{x})$. Then the right end of every segment $[a_k, b_k], [a_{k+1}, b_{k+1}], [a_{k+2}, b_{k+2}] \dots$ is less than \tilde{x} , it obviously contradicts to **[2]**.

We have a contradiction, so **[A]** is proved.

[B] We have to check that for any $\varepsilon > 0$ the set $(M - \varepsilon, M]$ contains at least one element of X . Let's assume that there exist some $\varepsilon > 0$ such that $(M - \varepsilon, M]$ does not contain any elements of X . Anyway, starting from some number k all the "left ends" a_n of the segments $[a_n, b_n]$ must belong to $(M - \varepsilon, M]$ and therefore, starting from some number k , every a_n is greater than any element of the set X , then every segment $[a_k, b_k], [a_{k+1}, b_{k+1}], [a_{k+2}, b_{k+2}] \dots$ does not contain any elements of X at all, it obviously contradicts to **[1]**. So **[B]** is proved.

From **[A]** and **[B]** follows that M is the least upper bound of X .

Similarly we can define:

Def3: a set X of real numbers is bounded below if there exist some number \tilde{m} such that $\forall x \in X: \tilde{m} \leq x$. In such case the number \tilde{m} is called "a lower bound of the set X ".

The definition of the greatest lower bound (or infimum) is similar, there is a similar criterion of the greatest lower bound and the similar theorem: any non-empty set X of real numbers, which is bounded below, has the greatest lower bound m . This theorem can be immediately derived from the least upper bound property (which we have proved). We just need to use the simple idea: m is a supremum of $X \Leftrightarrow -m$ is an infimum of $-X$.

Separability theorem. X and Y are set's of real numbers and any number of X is less than any number of Y , so for $\forall x \in X$ and for $\forall y \in Y$ we have $x < y$. Then there exist the number M such that $x \leq M \leq y \forall x \in X, \forall y \in Y$.

Proof. The set X is bounded above (by any element of the set Y), then X has a supremum M .

Let's show that $x \leq M \leq y \parallel \forall x \in X, \forall y \in Y$. The inequality $x \leq M$ is obvious.

Let's assume that there exist $\tilde{y} \in Y$ such that $\tilde{y} < M$. The half-interval $(\tilde{y}, M]$ must contain at least one element $\tilde{x} \in X$, then $\tilde{y} < \tilde{x}$ and we have a contradiction. Then $\forall y \in Y$ we have $M \leq y$.

Def. If some sequence is monotonically increasing **or** decreasing, then we say that the sequence is monotonic. When some set X is bounded above **and** below, we say that X is bounded.

Theorem [limit of a monotonic sequence]. $\{x_n\}$ is monotonic and bounded, then $\{x_n\}$ has a limit (then $\{x_n\}$ converges to some real number).

Proof. Let $\{x_n\}$ is monotonically increasing. As $\{x_n\}$ is bounded, the set of real numbers $X = \{x_j \mid j \in \mathbb{N}\}$ is bounded, then X has the least upper bound M . Let's show that $\lim x_n = M$. Let's fix an arbitrary positive $\varepsilon > 0$, the half interval $(M - \varepsilon, M]$ contains at least one term x_k , but $x_k \leq x_{k+1} \leq x_{k+2} \leq \dots \leq M$, then the set $(M - \varepsilon, M]$ contains all the terms of the sequence $\{x_n\}$, starting from the number k . Then a fortiori $(M - \varepsilon, M + \varepsilon) \equiv O_\varepsilon(M)$ contains all the terms of the sequence $\{x_n\}$, starting from the number k . So, for any positive $\varepsilon > 0$, the neighborhood $O_\varepsilon(M)$ contains all the terms of $\{x_n\}$, starting from some number, it means that $\lim x_n = M$. And there is a similar proof for any monotonically decreasing sequence $\{x_n\}$, but we have to consider the set $X = \{x_j \mid j \in \mathbb{N}\}$ and the greatest lower bound m of X . And similarly (as above), we can show that $\lim x_n = m$.

Def. The least upper bound of X (or a supremum) can be denoted as $\sup X$. The greatest lower bound of X (or an infimum) can be denoted as $\inf X$.

Decimal notation of real numbers

Assertion1. Let $\{x_n\} \rightarrow a$ and $\{y_n\} \rightarrow b$.

[1-st part] If there exist some $\varepsilon > 0$ such that starting from some number $k \in \mathbb{N}$ we have

$$y_{k+1} - x_{k+1} > \varepsilon, y_{k+2} - x_{k+2} > \varepsilon, y_{k+3} - x_{k+3} > \varepsilon \dots, \text{ then } b > a.$$

[2-nd part] If $b > a$, then there exist some $\varepsilon > 0$ such that starting from some number $k \in \mathbb{N}$ we have $y_{k+1} - x_{k+1} > \varepsilon, y_{k+2} - x_{k+2} > \varepsilon, y_{k+3} - x_{k+3} > \varepsilon \dots$

Proof. [1-st part] we have here $y_{k+1} > x_{k+1} + \varepsilon, y_{k+2} > x_{k+2} + \varepsilon, y_{k+3} > x_{k+3} + \varepsilon \dots$

As $\{x_n\} \rightarrow a$, then for $\varepsilon/2 > 0$, starting from some number $p : \forall n > p$ we have $-\varepsilon/2 < x_n - a < \varepsilon/2$.

As $\{y_n\} \rightarrow b$, then for $\varepsilon/2 > 0$, starting from some number $m : \forall n > m$ we have $-\varepsilon/2 < y_n - b < \varepsilon/2$.

Let's take $j \equiv \max(p, m, k)$ then for any $n > j$ we have:

$-\varepsilon/2 < x_n - a < \varepsilon/2$ and $-\varepsilon/2 < y_n - b < \varepsilon/2$ and $y_n > x_n + \varepsilon$. Let's rewrite it like:

[1] $a - \varepsilon/2 < x_n < a + \varepsilon/2$ and **[2]** $b - \varepsilon/2 < y_n < b + \varepsilon/2$ and **[3]** $y_n > x_n + \varepsilon$.

From **[3]** and **[2]** follows that $x_n + \varepsilon < b + \varepsilon/2 \Rightarrow x_n < (b - \varepsilon/2)$ from this inequality and **[1]** we have $a - \varepsilon/2 < b - \varepsilon/2$, then $a < b$.

[2-nd part] $b > a$, let's take $\varepsilon \equiv (b - a)$. As $\{x_n\} \rightarrow a$, then there exist $p : \forall n > p$ we have

$-\varepsilon/3 < x_n - a < \varepsilon/3$. As $\{y_n\} \rightarrow b$, then there exist $m : \forall n > m$ we have $-\varepsilon/3 < y_n - b < \varepsilon/3$.

Let's take $k \equiv \max(p, m)$. Then for any $n > k$ we have: $-\varepsilon/3 < x_n - a < \varepsilon/3$ and

$-\varepsilon/3 < y_n - b < \varepsilon/3$.

Let's rewrite these inequalities: **[1]** $a - \varepsilon/3 < x_n < a + \varepsilon/3$ and **[2]** $b - \varepsilon/3 < y_n < b + \varepsilon/3$.

Let's notice that $a + \varepsilon/3 < b - \varepsilon/3$, then we have: $a - \varepsilon/3 < x_n < a + \varepsilon/3 < b - \varepsilon/3 < y_n < b + \varepsilon/3$

from here: $y_n - x_n > (b - \varepsilon/3) - (a + \varepsilon/3) = (b - a) - 2\varepsilon/3 = \varepsilon/3$. So, for any $n > k$ we have

$y_n - x_n > \varepsilon/3 \equiv \text{const} > 0$.

Let's sum up. If $b > a$, then $y_n - x_n$ is greater than some positive ε (starting from some number k).

And conversely, if $y_n - x_n$ is greater than some positive ε (starting from some number k), then $b > a$.

Consequence1. If $x_n \leq y_n \forall n$ and both sequences $\{x_n\}$ and $\{y_n\}$ converge. Then $\lim x_n \leq \lim y_n$.

Proof. Let's assume that $\lim x_n > \lim y_n$, then we have $x_n - y_n > \varepsilon > 0$ starting from some number k , then $x_n > y_n$ (for $n > k$), it contradicts to the initial requirement $x_n \leq y_n \forall n$.

Therefore $\lim x_n \leq \lim y_n$.

Notice, if $x_n < y_n \forall n$ we can't guarantee that $\lim x_n < \lim y_n$ (when both sequences $\{x_n\}, \{y_n\}$ converge) we can only guarantee that $\lim x_n \leq \lim y_n$.

Consider for example $x_n = 1 - \frac{1}{n}$ and $y_n = 1 - \frac{1}{2n}$, we have here $x_n < y_n \forall n$ and $\lim x_n = \lim y_n = 1$. In order to claim that $\lim x_n < \lim y_n$ we need to have a condition like $y_n - x_n > \varepsilon > 0$ (starting from some k).

Def. Let $\{a_n\}$ is any sequence of real numbers. The symbol $\sum_{n=1}^{+\infty} a_n$ is called a series.

For any $n \in \mathbb{N}$ the sum $S_n \equiv a_1 + a_2 + \dots + a_n$ is called a partial sum of the series $\sum_{n=1}^{+\infty} a_n$.

We say that $\sum_{n=1}^{+\infty} a_n$ converges to S (or goes to S) and we write $\sum_{n=1}^{+\infty} a_n = S$ if the sequence of partial sums $\{S_n\}$ goes to S .

The number S in such case is called a sum of the series $\sum_{n=1}^{+\infty} a_n$.

So, when we look at some series $\sum_{n=1}^{+\infty} a_n$ we should perceive it as a sequence of it's partial sums

$(a_1), (a_1 + a_2), (a_1 + a_2 + a_3), (a_1 + a_2 + a_3 + a_4) \dots$. And the writing $\sum_{n=1}^{+\infty} a_n = S$ means that this sequence of partial sums goes to S .

If the sequence of partial sums $(a_1), (a_1 + a_2), (a_1 + a_2 + a_3), (a_1 + a_2 + a_3 + a_4) \dots$ does not have any limit, then we say that $\sum_{n=1}^{+\infty} a_n$ diverges.

When $\sum_{n=1}^{+\infty} a_n = S$ we can also write it as $a_1 + a_2 + a_3 + \dots = S$. If we write $\sum_{n=1}^{+\infty} a_n < \sum_{n=1}^{+\infty} b_n$, we mean

that both series $\sum_{n=1}^{+\infty} a_n$ and $\sum_{n=1}^{+\infty} b_n$ converge, and the sum of the series $\sum_{n=1}^{+\infty} a_n$ is less than the sum

of the series $\sum_{n=1}^{+\infty} b_n$. And similarly for $\sum_{n=1}^{+\infty} a_n \leq \sum_{n=1}^{+\infty} b_n$.

From now on we consider **only non-negative** serieses $\sum_{n=1}^{+\infty} a_n \parallel a_n \geq 0 \forall n$.

Lemma 1. A non-negative series $\sum_{n=1}^{+\infty} a_n$ converges \Leftrightarrow The set of it's partial sums $\left\{ \sum_{n=1}^m a_n \right\}$ is bounded above.

Proof. \Rightarrow Let $\sum_{n=1}^{+\infty} a_n$ converges.

Let's denote: $S_1 \equiv a_1$, $S_2 \equiv a_1 + a_2$, $S_3 \equiv a_1 + a_2 + a_3$, $S_4 \equiv a_1 + a_2 + a_3 + a_4$, the sequence $\{S_n\}$

is monotonically increasing, and it has some limit S (because $\sum_{n=1}^{+\infty} a_n$ converges).

According to [auxiliary1](#) (page 110), we have $S_n \leq S \forall n$. Then the set of all partial sums is bounded above by S .

Conversely. \Leftarrow Let the set of partial sums is bounded above, it means that the sequence $\{S_n\}$ is bounded. The sequence $\{S_n\}$ is monotonically increasing (because we have a non-negative series). Then (according to the theorem about a limit of a monotonic sequence) $\{S_n\}$ converges,

it means that $\sum_{n=1}^{+\infty} a_n$ converges.

Lemma2. $\sum_{n=1}^{+\infty} b_n$ converges and $a_n \leq b_n \forall n$, then **[A]** $\sum_{n=1}^{+\infty} a_n$ also converges and **[B]** $\sum_{n=1}^{+\infty} a_n \leq \sum_{n=1}^{+\infty} b_n$.

[C] If there exist just one number $\bar{k} \in \mathbb{N}$ such that $a_{\bar{k}} < b_{\bar{k}}$, then $\sum_{n=1}^{+\infty} a_n < \sum_{n=1}^{+\infty} b_n$.

Notice. In **[C]** we claim that: if there exist just one (any one) number \bar{k} , for which $a_{\bar{k}}$ is strictly less than $b_{\bar{k}}$, then the whole sum of the series $\sum_{n=1}^{+\infty} a_n$ is strictly less than the sum of the series $\sum_{n=1}^{+\infty} b_n$.

Proof. Let $\tilde{S}_n \equiv b_1 + \dots + b_n$ and $S_n \equiv a_1 + \dots + a_n$. As $\sum_{n=1}^{+\infty} b_n$ converges ([lemma1](#)) the set of partial

sums $\{\tilde{S}_n \mid n \in \mathbb{N}\}$ is bounded above. As $S_n \leq \tilde{S}_n \mid \forall n$, the set of partial sums of $\sum_{n=1}^{+\infty} a_n$ is also

bounded above. Then $\sum_{n=1}^{+\infty} a_n$ converges ([lemma1](#)) (and **[A]** is proved). The sum S of the series $\sum_{n=1}^{+\infty} a_n$

is a limit of the sequence $\{S_n\}$ and the sum \tilde{S} of the series $\sum_{n=1}^{+\infty} b_n$ is a limit of the sequence $\{\tilde{S}_n\}$,

we have $S_n \leq \tilde{S}_n \mid \forall n$, then ([consequence1](#)) $S \leq \tilde{S}$ it means exactly that $\sum_{n=1}^{+\infty} a_n \leq \sum_{n=1}^{+\infty} b_n$

(and **[B]** is proved).

Let now there exist $\bar{k} \in \mathbb{N}$ such that $a_{\bar{k}} < b_{\bar{k}}$, then

$$\tilde{S}_{\bar{k}} - S_{\bar{k}} = (b_1 + b_2 + \dots + b_{\bar{k}}) - (a_1 + a_2 + \dots + a_{\bar{k}}) \geq b_{\bar{k}} - a_{\bar{k}} > \frac{b_{\bar{k}} - a_{\bar{k}}}{2} \equiv \varepsilon = \text{const}. \text{ For any } n > \bar{k}$$

we obviously have $\tilde{S}_n - S_n > \varepsilon > 0$. Then ([assertion1](#)) $\lim \tilde{S}_n > \lim S_n \Leftrightarrow \sum_{n=1}^{+\infty} b_n > \sum_{n=1}^{+\infty} a_n$.

Everything is proved.

Lemma3 [sum of a geometric progression]. For any $q \in R \parallel q \neq 1$ the next formula is true:

$$1 + q + q^2 + \dots + q^n = \frac{q^{n+1} - 1}{q - 1}.$$

Proof: The given formula is equivalent to $(1 + q + q^2 + \dots + q^n) \cdot (q - 1) = q^{n+1} - 1$ and this one is very easy to check, we just need to simplify the expression ("expand the brackets") on the left side.

Consequence2. For any $a, q \in R \parallel q \neq 1$ we have $a + aq + aq^2 + \dots + aq^n = \frac{a(q^{n+1} - 1)}{q - 1}$.

Lemma3. For any $q \in R \parallel |q| < 1$ we have $\lim_{n \rightarrow \infty} q^n = 0$.

Proof. In order to prove this one we have to prove a very important auxiliary inequality, which we will also use in the future.

Auxiliary [Bernoulli inequality]. For any $\forall n \in \mathbb{N}, \forall x \geq -1$ the next inequality is true:

$$(1 + x)^n \geq 1 + nx.$$

Proof. By induction: $n = 1$, then the inequality is obviously true. If the inequality is true for some $k \in \mathbb{N}$, then $(1 + x)^k \geq 1 + kx$. Let's consider

$$(1 + x)^{k+1} = (1 + x)^k \cdot (1 + x) \geq (1 + kx) \cdot (1 + x) = 1 + x + kx + kx^2 = 1 + (k + 1)x + kx^2 \geq 1 + (k + 1)x.$$

So, the inequality is true for $(k + 1) \in \mathbb{N}$. Everything is proved.

Notice: the requirement $x \geq -1$ is important, it guarantees that $1 + x \geq 0$ which allows us to write:
 " $(1 + x)^k \cdot (1 + x) \geq (1 + kx) \cdot (1 + x)$ ".

Let's prove the lemma3. If we can show that $\lim_{n \rightarrow \infty} |q|^n = 0$, then $\lim_{n \rightarrow \infty} q^n = 0$. Really, for any n we have $0 \leq q^n \leq |q|^n$ and if $\{|q|^n\} \rightarrow 0$, then, according to the squeeze theorem for sequences, $\{q^n\} \rightarrow 0$.

Let's represent $|q| < 1$ as a ratio $|q| = \frac{1}{1 + h}$ (Where $h \equiv \frac{1}{|q|} - 1 > 0$, so $h = \text{const} > 0$).

Then $|q|^n = \frac{1}{(1 + h)^n} \leq \left[\begin{array}{c} \text{Bernoulli} \\ \text{inequality} \end{array} \right] \leq \frac{1}{1 + nh} < \frac{1}{nh}$. Then we have $0 \leq |q|^n \leq \frac{1}{nh}$ and

(squeeze theorem for sequences), from $\{0\} \rightarrow 0$ and $\left\{ \frac{1}{nh} \right\} \rightarrow 0$ follows that $\{|q|^n\} \rightarrow 0$.

Lemma4 [sum of a geometric series]. For any $q \in R \parallel |q| < 1$ the next formula is true:

$$1 + q + q^2 + \dots + q^n + \dots = \frac{1}{1 - q}.$$

Proof. Here we speak about the sum of the series, the partial sum here ([lemma3](#)) is

$$S_n = 1 + q + \dots + q^{n-1} = \frac{q^n - 1}{q - 1}. \text{ We want to find}$$

$$\begin{aligned} \lim_{n \rightarrow \infty} S_n &= \lim_{n \rightarrow \infty} \frac{q^n - 1}{q - 1} = \lim_{n \rightarrow \infty} \frac{1}{q - 1} \cdot (q^n - 1) = \lim_{n \rightarrow \infty} \frac{1}{q - 1} \cdot \lim_{n \rightarrow \infty} (q^n - 1) = \\ &= \frac{1}{q - 1} \cdot (-1) = \frac{1}{1 - q}. \end{aligned}$$

Consequence3. For any $a, q \in R \parallel |q| < 1$ we have $a + aq + aq^2 + \dots + aq^n + \dots = \frac{a}{1 - q}$.

Notice. We have used above $\lim a_n \cdot b_n = \lim a_n \cdot \lim b_n$. Remember that we can do so **only when** both limits $\lim a_n$ and $\lim b_n$ do exist. Unless we aren't sure that both limits $\lim a_n$ and $\lim b_n$ do exist, we can't perform this action. Similarly, when we carry out any of the next actions, $\lim(a_n \pm b_n) = \lim a_n \pm \lim b_n$ or $\lim(a_n / b_n) = \lim a_n / \lim b_n$, we need to make sure at first that both limits $\lim a_n$ and $\lim b_n$ do exist (in the last case we also need $\lim b_n \neq 0$ and $b_n \neq 0 \forall n$).

Def. A sequence of integer numbers $d_1, d_2, d_3, \dots \parallel 0 \leq d_n \leq 9 \forall n$ is called "allowable" if it is not a zero sequence $0, 0, 0, 0, \dots$ and there is no any $\bar{k} \in \mathbb{N}$ such that $d_n = 9 \forall n \geq \bar{k}$.

Once again, there is a sequence which consists of integer numbers from 0 to 9. This sequence is called allowable if it is not a zero sequence, and it does not have a "9-tail" like $9, 9, 9, 9, \dots$.

From now on we consider only allowable sequences.

Assertion2. For any allowable sequence d_1, d_2, d_3, \dots the series $\frac{d_1}{10^1} + \frac{d_2}{10^2} + \dots + \frac{d_m}{10^m} + \dots = \sum_{n=1}^{+\infty} \frac{d_n}{10^n}$ converges, and the sum of such series is a number $S \in (0, 1)$.

Proof. Let's fix any allowable sequence d_1, d_2, d_3, \dots and let's take the sequence $9, 9, 9, 9, \dots$.

$$\text{Let's consider the series } \frac{9}{10^1} + \frac{9}{10^2} + \dots + \frac{9}{10^m} + \dots = // \text{consequence 3} // = \frac{9}{1 - 1/10} = 1.$$

As d_1, d_2, d_3, \dots is allowable, then $d_n \leq 9 \forall n$ and there exist \bar{k} such that $d_{\bar{k}} < 9$.

$$\text{So we have: } \frac{d_n}{10^n} \leq \frac{9}{10^n} \forall n \text{ and there exist } \bar{k} \text{ such that } \frac{d_{\bar{k}}}{10^{\bar{k}}} < \frac{9}{10^{\bar{k}}}.$$

Then any term (with number k) of the series $\frac{d_1}{10^1} + \frac{d_2}{10^2} + \dots + \frac{d_m}{10^m} + \dots = \sum_{n=1}^{+\infty} \frac{d_n}{10^n}$ is not greater than

any term (with number k) of the series $\frac{9}{10^1} + \frac{9}{10^2} + \dots + \frac{9}{10^m} + \dots$, and the \bar{k} -th term of the first

series is strictly less than the $\bar{k} - th$ term of the second series. Then ([lemma2](#)) the first series converges and it's sum is less than the sum of the second series, which is equal to 1. So $\sum_{n=1}^{+\infty} \frac{d_n}{10^n} < 1$.

Next: the sum of the zero series $\frac{0}{10^1} + \frac{0}{10^2} + \dots + \frac{0}{10^m} + \dots$ is equal to zero. As d_1, d_2, d_3, \dots is allowable, then there exist $\bar{m} \in \mathbb{N}$ such that $d_{\bar{m}} > 0$. Let's compare the zero series with the series $\frac{d_1}{10^1} + \frac{d_2}{10^2} + \dots + \frac{d_{\bar{m}}}{10^{\bar{m}}} + \dots$. We have $0 \leq d_n \forall n$ and $\exists \bar{m} \in \mathbb{N} : 0 < d_{\bar{m}}$.

Then ([lemma2](#)) $\sum_{n=1}^{+\infty} \frac{0}{10^n} < \sum_{n=1}^{+\infty} \frac{d_n}{10^n} \Rightarrow 0 < \sum_{n=1}^{+\infty} \frac{d_n}{10^n}$. We have deduced that $0 < \sum_{n=1}^{+\infty} \frac{d_n}{10^n} < 1$.

The main theorem. Let Ω is a set of all allowable sequences d_1, d_2, d_3, \dots . There exist one-to-one mapping $f : \Omega \rightarrow (0,1)$: for every allowable sequence d_1, d_2, d_3, \dots it compares the unique real number $P_1 \in (0,1)$ which is a sum of the series $\sum_{n=1}^{+\infty} \frac{d_n}{10^n}$.

Proof. The mapping f is defined like $f(d_1, d_2, d_3, \dots) = \sum_{n=1}^{+\infty} \frac{d_n}{10^n}$.

From the [assertion2](#) follows that f is really a mapping from Ω to $(0,1)$.

[PART 1] Let's show that f fully covers the set $(0,1)$. Let's fix an arbitrary $P_1 \in (0,1)$.

Let's build the sequence of pairs of **natural** numbers $(m_1, k_1), (m_2, k_2), (m_3, k_3) \dots$ where $1 \leq m_j \leq 9 \forall j$.

[Step1] For $P_1 \in (0,1)$ there exist the minimal natural number k_1 such that $\frac{1}{10^{k_1}} \leq P_1$

(it's easy to show, by using the **Archimedes axiom** and **induction**). Let's fix this number k_1 .

As k_1 is a minimal number with such property, then $\frac{1}{10^{k_1}} \leq P_1 < \frac{1}{10^{k_1-1}}$. **Next**, for the positive

numbers $\frac{1}{10^{k_1}}$, P_1 there exist the maximal natural number m_1 such that $\frac{m_1}{10^{k_1}} \leq P_1$ (it follows from

the **Archimedes axiom**). Then: $\frac{m_1}{10^{k_1}} \leq P_1 < \frac{1}{10^{k_1-1}}$. There must be $1 \leq m_1 \leq 9$ (really, the assumption

$m_1 \geq 10$, contradicts the inequality $\frac{m_1}{10^{k_1}} \leq P_1 < \frac{1}{10^{k_1-1}}$).

Let's also notice that $\frac{m_1}{10^{k_1}} \leq P_1 < \frac{m_1+1}{10^{k_1}}$ **[J]** (because m_1 is a maximal number such that $\frac{m_1}{10^{k_1}} \leq P_1$).

Let's subtract $\frac{m_1}{10^{k_1}}$ from all sides of **[J]**, we will get $0 \leq \left(P_1 - \frac{m_1}{10^{k_1}} \right) < \frac{1}{10^{k_1}}$.

If $0 = P_1 - \frac{m_1}{10^{k_1}}$, then we fix the pair (m_1, k_1) and end the process.

If $0 < P_1 - \frac{m_1}{10^{k_1}}$, then we designate $P_2 \equiv P_1 - \frac{m_1}{10^{k_1}}$ and we have $0 < P_2 < \frac{1}{10^{k_1}} \Rightarrow P_2 \in (0,1)$ and we repeat the **[Step1]** for the number P_2 .

We will find the pair of natural numbers (m_2, k_2) . At first we will find k_2 such that $\frac{1}{10^{k_2}} \leq P_2$, notice that $k_1 < k_2$ (because we already have $P_2 < \frac{1}{10^{k_1}}$). Then $\frac{m_2}{10^{k_2}} \leq P_2 < \frac{1}{10^{k_2-1}}$ from here follows that $1 \leq m_2 \leq 9$, and finally $0 \leq \left(P_2 - \frac{m_2}{10^{k_2}} \right) < \frac{1}{10^{k_2}}$.

If $0 = P_2 - \frac{m_2}{10^{k_2}}$, then we fix the pairs (m_1, k_1) , (m_2, k_2) and end the process.

If $0 < P_2 - \frac{m_2}{10^{k_2}}$, then we designate $P_3 \equiv P_2 - \frac{m_2}{10^{k_2}}$. And we repeat the **[Step1]** for the number P_3 .

We will get the pair (m_3, k_3) such that $k_1 < k_2 < k_3 < \dots$ and $1 \leq m_3 \leq 9$.

And so on. For any pair (m_p, k_p) we have $0 \leq \left(P_p - \frac{m_p}{10^{k_p}} \right) < \frac{1}{10^{k_p}}$.

[1-st case] If the process has ended in p steps, then we get $0 = \left(P_p - \frac{m_p}{10^{k_p}} \right)$ and we have fixed some pairs (m_1, k_1) , $(m_2, k_2) \dots (m_p, k_p)$. Here everywhere $1 \leq m_j \leq 9$ and $k_1 < k_2 < \dots < k_p \in \mathbb{N}$.

Let's remember that: $P_p \equiv P_{p-1} - \frac{m_{p-1}}{10^{k_{p-1}}} \parallel P_{p-1} \equiv P_{p-2} - \frac{m_{p-2}}{10^{k_{p-2}}} \parallel P_{p-2} \equiv P_{p-3} - \frac{m_{p-3}}{10^{k_{p-3}}} \parallel \dots$

$\dots \parallel P_3 \equiv P_2 - \frac{m_2}{10^{k_2}}, \parallel P_2 \equiv P_1 - \frac{m_1}{10^{k_1}} \parallel$, then $P_p = P_1 - \frac{m_1}{10^{k_1}} - \frac{m_2}{10^{k_2}} - \frac{m_3}{10^{k_3}} - \dots - \frac{m_{p-1}}{10^{k_{p-1}}}$ **[F]**

in addition to it, we also have: $0 = \left(P_p - \frac{m_p}{10^{k_p}} \right)$, then we have

$$P_1 = \frac{m_1}{10^{k_1}} + \frac{m_2}{10^{k_2}} + \frac{m_3}{10^{k_3}} + \dots + \frac{m_{p-1}}{10^{k_{p-1}}} + \frac{m_p}{10^{k_p}}.$$

[2-nd case] The process hasn't ended in p steps. Then we have some sequence

(m_1, k_1) , $(m_2, k_2) \dots (m_p, k_p) \dots$ here everywhere $1 \leq m_j \leq 9$ and $k_1 < k_2 < \dots < k_p < \dots \in \mathbb{N}$.

Let's show that the series $\frac{m_1}{10^{k_1}} + \frac{m_2}{10^{k_2}} + \frac{m_3}{10^{k_3}} + \dots \equiv \sum_{j=1}^{+\infty} \frac{m_j}{10^{k_j}}$ converges to P_1 . We got above the

simple formula **[F]** $P_p = P_1 - \frac{m_1}{10^{k_1}} - \frac{m_2}{10^{k_2}} - \frac{m_3}{10^{k_3}} - \dots - \frac{m_{p-1}}{10^{k_{p-1}}}$ (for any $p \in \mathbb{N}$), then

$$\frac{m_1}{10^{k_1}} + \frac{m_2}{10^{k_2}} + \frac{m_3}{10^{k_3}} + \dots + \frac{m_{p-1}}{10^{k_{p-1}}} = P_1 - P_p \quad \text{[T].}$$

Let's add $\frac{m_p}{10^{k_p}}$ to both sides of **[T]** and use the inequality $0 \leq \left(P_p - \frac{m_p}{10^{k_p}} \right) < \frac{1}{10^{k_p}}$ **[E]**

(we have such inequality for every P_p). So:

$$\begin{aligned} \frac{m_1}{10^{k_1}} + \frac{m_2}{10^{k_2}} + \frac{m_3}{10^{k_3}} + \dots + \frac{m_{p-1}}{10^{k_{p-1}}} + \frac{m_p}{10^{k_p}} &= P_1 - P_p + \frac{m_p}{10^{k_p}} \Leftrightarrow \\ \Leftrightarrow \frac{m_1}{10^{k_1}} + \frac{m_2}{10^{k_2}} + \frac{m_3}{10^{k_3}} + \dots + \frac{m_{p-1}}{10^{k_{p-1}}} + \frac{m_p}{10^{k_p}} &= P_1 - \left(P_p - \frac{m_p}{10^{k_p}} \right). \text{ Let's regroup the summands} \\ \left(P_p - \frac{m_p}{10^{k_p}} \right) &= P_1 - \left(\frac{m_1}{10^{k_1}} + \frac{m_2}{10^{k_2}} + \frac{m_3}{10^{k_3}} + \dots + \frac{m_{p-1}}{10^{k_{p-1}}} + \frac{m_p}{10^{k_p}} \right). \end{aligned}$$

According to **[E]**: $0 \leq P_1 - \left(\frac{m_1}{10^{k_1}} + \frac{m_2}{10^{k_2}} + \frac{m_3}{10^{k_3}} + \dots + \frac{m_{p-1}}{10^{k_{p-1}}} + \frac{m_p}{10^{k_p}} \right) < \frac{1}{10^{k_p}}$ **[E]**.

We have the estimation for $P_1 - \left(\text{the partial sum of } \sum_{j=1}^{+\infty} \frac{m_j}{10^{k_j}} \text{ with } p \text{ summands} \right)$.

Both sequences $\{x_p\} \equiv \{0\} \equiv 0, 0, 0, \dots$ and $\{z_p\} \equiv \left\{ \frac{1}{10^{k_p}} \right\}$ are infinitely small, then, according to the

squeeze theorem for sequences, $\left\{ P_1 - \left(\frac{m_1}{10^{k_1}} + \frac{m_2}{10^{k_2}} + \frac{m_3}{10^{k_3}} + \dots + \frac{m_{p-1}}{10^{k_{p-1}}} + \frac{m_p}{10^{k_p}} \right) \right\}$ is infinitely small.

It means exactly that our series $\sum_{n=1}^{+\infty} \frac{m_j}{10^{k_j}}$ goes to P_1 .

Let's sum up: from the **1-st** case and **2-nd** case follows that any number $P_1 \in (0,1)$ can be represented as a finite or an infinite sum $P_1 = \frac{m_1}{10^{k_1}} + \frac{m_2}{10^{k_2}} + \frac{m_3}{10^{k_3}} + \dots + \frac{m_{p-1}}{10^{k_{p-1}}} + \frac{m_p}{10^{k_p}} + \dots$, where $1 \leq m_j \leq 9$ and $k_1 < k_2 < \dots < k_p < \dots \in \mathbb{N}$. Notice that $k_1 < k_2 < \dots < k_p < \dots$ are not necessary consecutive natural numbers.

Let's show that: if P_1 is represented as a sum of a series, the next situation is impossible:

from some moment all the numbers $k_{p+1} < k_{p+2} < k_{p+3} < \dots$ are consecutive natural numbers and all the numbers $m_{p+1}, m_{p+2}, m_{p+3}, \dots$ are equal to 9. Let's assume the contrary, then we have the

representation: $P_1 = \frac{m_1}{10^{k_1}} + \dots + \frac{m_p}{10^{k_p}} + \frac{9}{10^{k_p+1}} + \frac{9}{10^{k_p+2}} + \frac{9}{10^{k_p+3}} + \dots$ [V]. Let's denote

$S_p \equiv \frac{m_1}{10^{k_1}} + \dots + \frac{m_p}{10^{k_p}}$. From [E] we have $0 \leq P_1 - S_p < \frac{1}{10^{k_p}}$, then $P_1 - S_p = \frac{1}{10^{k_p}} - \varepsilon \parallel \varepsilon > 0$ [J].

From [V] we see that P_1 is a limit of the sequence

$\left(S_p + \frac{9}{10^{k_p+1}}\right), \left(S_p + \frac{9}{10^{k_p+1}} + \frac{9}{10^{k_p+2}}\right), \left(S_p + \frac{9}{10^{k_p+1}} + \frac{9}{10^{k_p+2}} + \frac{9}{10^{k_p+3}}\right) \dots$ [P]. This sequence is

a sum of the sequences $\{a_n\} \equiv S_p, S_p, S_p \dots$ (here $\lim_{n \rightarrow \infty} a_n = S_p$) and

$\{b_n\} \equiv \left(\frac{9}{10^{k_p+1}}\right), \left(\frac{9}{10^{k_p+1}} + \frac{9}{10^{k_p+2}}\right), \left(\frac{9}{10^{k_p+1}} + \frac{9}{10^{k_p+2}} + \frac{9}{10^{k_p+3}}\right) \dots$ (and here $\lim_{n \rightarrow \infty} b_n = \frac{1}{10^{k_p}}$,

because $\lim_{n \rightarrow \infty} b_n$ is a sum of the geometric series). The limit of the sequence [P] is a sum of limits

$\lim_{n \rightarrow \infty} a_n + \lim_{n \rightarrow \infty} b_n = S_p + \frac{1}{10^{k_p}}$. Then $P_1 = S_p + \frac{1}{10^{k_p}}$, but from [J] we have

$P_1 = S_p + \frac{1}{10^{k_p}} - \varepsilon \parallel \varepsilon > 0$ and we have a contradiction.

And finally, let's define the series $\sum_{n=1}^{+\infty} \frac{d_n}{10^n}$ that "coincides" with the finite or infinite sum

$\frac{m_1}{10^{k_1}} + \frac{m_2}{10^{k_2}} + \frac{m_3}{10^{k_3}} + \dots = P_1$. We have concrete natural numbers $k_1 < k_2 < \dots < k_p < \dots \in \mathbb{N}$.

For every natural number n which differs from any of these numbers: $n \neq k_j \forall j$ we define $d_n \equiv 0$,

and the summand $\frac{d_n}{10^n} = 0$ in this case. And for every natural number n which is some k_j , i.e.,

$n = k_j$ (for some j), we define $d_n \equiv m_j$, so the summand $\frac{d_n}{10^n} = \frac{m_j}{10^{k_j}}$ in this case.

Then the series $\sum_{n=1}^{+\infty} \frac{d_n}{10^n}$ "coincides" with the finite or infinite sum $\frac{m_1}{10^{k_1}} + \frac{m_2}{10^{k_2}} + \frac{m_3}{10^{k_3}} + \dots$ and

therefore $\sum_{n=1}^{+\infty} \frac{d_n}{10^n}$ goes to P_1 . So $\sum_{n=1}^{+\infty} \frac{d_n}{10^n} = P_1$. The sequence d_1, d_2, d_3, \dots is **allowable**.

Really, $\forall j \Rightarrow 0 \leq d_j \leq 9$. Let's notice that d_1, d_2, d_3, \dots is not a zero sequence, because all

$m_1, m_2, m_3 \dots$ are natural. And also d_1, d_2, d_3, \dots does not have a tail 9,9,9,9...

(because $m_1, m_2, m_3 \dots$ does not have such tail, as we showed above).

So, for any $P_1 \in (0,1)$ there exist the allowable sequence $d_1, d_2, d_3, \dots \in \Omega$ such that

$$f(d_1, d_2, d_3, \dots) = \sum_{n=1}^{+\infty} \frac{d_n}{10^n} = P_1, \text{ we have proved that the mapping } f \text{ fully covers the set } (0,1).$$

[PART 2] Let's show that f doesn't glue together elements of Ω . Let's assume that for different allowable sequences $d_1, d_2, d_3, \dots \neq a_1, a_2, a_3, \dots$ we have

$$f(d_1, d_2, d_3, \dots) = f(a_1, a_2, a_3, \dots) \Leftrightarrow \sum_{n=1}^{+\infty} \frac{d_n}{10^n} = \sum_{n=1}^{+\infty} \frac{a_n}{10^n}. \text{ Let's compare } d_1 \text{ and } a_1, \text{ if } d_1 = a_1, \text{ then we go}$$

to d_2 and a_2 . If $d_2 = a_2$, then we compare d_3 and a_3 and etc. As the sequences d_1, d_2, d_3, \dots and a_1, a_2, a_3, \dots are different, then there exist $m \in \mathbb{N}$ such that

$$d_1 = a_1, d_2 = a_2, \dots, d_{m-1} = a_{m-1}, d_m \neq a_m \text{ (maybe } m=1 \text{ and we have } d_1 \neq a_1 \text{ from the start)}.$$

Without loss of generality $d_m \neq a_m \Rightarrow a_m < d_m$. In several consecutive steps we will show that

$$\sum_{n=1}^{+\infty} \frac{a_n}{10^n} < \sum_{n=1}^{+\infty} \frac{d_n}{10^n}. \text{ Really, as the sequence } a_1, a_2, a_3, \dots \text{ does not have a } 9,9,9, \dots \text{ tail, then (lemma2)}$$

$$\sum_{n=1}^{+\infty} \frac{a_n}{10^n} < \frac{a_1}{10} + \dots + \frac{a_m}{10^m} + \frac{9}{10^{m+1}} + \frac{9}{10^{m+2}} + \frac{9}{10^{m+3}} + \dots. \text{ Let's denote } \Sigma_m \equiv \frac{a_1}{10} + \dots + \frac{a_m}{10^m}, \text{ then the}$$

sum of the last series is a limit of the sequence

$$\left\{ \Sigma_m + \frac{9}{10^{m+1}} \right\}, \left\{ \Sigma_m + \frac{9}{10^{m+1}} + \frac{9}{10^{m+2}} \right\}, \left\{ \Sigma_m + \frac{9}{10^{m+1}} + \frac{9}{10^{m+2}} + \frac{9}{10^{m+3}} \right\}, \text{ this sequence is a sum of}$$

$$\text{sequences } \{a_n\} \equiv \Sigma_m, \Sigma_m, \Sigma_m, \dots \text{ and } \{b_n\} \equiv \left(\frac{9}{10^{m+1}} \right), \left(\frac{9}{10^{m+1}} + \frac{9}{10^{m+2}} \right), \left(\frac{9}{10^{m+1}} + \frac{9}{10^{m+2}} + \frac{9}{10^{m+3}} \right) \dots$$

and $\lim_{n \rightarrow \infty} b_n$ is a sum of the geometric series, so $\lim_{n \rightarrow \infty} b_n = \frac{1}{10^m}$ and $\lim_{n \rightarrow \infty} a_n = \Sigma_m$, then

$$\frac{a_1}{10} + \dots + \frac{a_m}{10^m} + \frac{9}{10^{m+1}} + \frac{9}{10^{m+2}} + \frac{9}{10^{m+3}} + \dots = \Sigma_m + \frac{1}{10^m} = \left(\frac{a_1}{10} + \dots + \frac{a_{m-1}}{10^{m-1}} + \frac{a_m}{10^m} \right) + \frac{1}{10^m} =$$

$$// \text{ as } a_1 = d_1 \dots a_{m-1} = d_{m-1} // = \left(\frac{d_1}{10} + \dots + \frac{d_{m-1}}{10^{m-1}} + \frac{a_m}{10^m} \right) + \frac{1}{10^m} = \frac{d_1}{10} + \dots + \frac{d_{m-1}}{10^{m-1}} + \frac{a_m + 1}{10^m} \leq$$

$$\leq \left[\begin{array}{l} a_m < d_m \Rightarrow \\ \Rightarrow a_m + 1 \leq d_m \end{array} \right] \leq \frac{d_1}{10} + \dots + \frac{d_{m-1}}{10^{m-1}} + \frac{d_m}{10^m} = \frac{d_1}{10} + \dots + \frac{d_{m-1}}{10^{m-1}} + \frac{d_m}{10^m} + \frac{0}{10^{m+1}} + \frac{0}{10^{m+2}} + \dots$$

$$\leq // \text{ Lemma2 } // \leq \frac{d_1}{10} + \dots + \frac{d_{m-1}}{10^{m-1}} + \frac{d_m}{10^m} + \frac{d_{m+1}}{10^{m+1}} + \frac{d_{m+2}}{10^{m+2}} + \dots = \sum_{n=1}^{+\infty} \frac{d_n}{10^n}$$

So, in several steps we have deduced that $\sum_{n=1}^{+\infty} \frac{a_n}{10^n} < \sum_{n=1}^{+\infty} \frac{d_n}{10^n}$ - it contradicts to our initial assumption

$$\sum_{n=1}^{+\infty} \frac{d_n}{10^n} = \sum_{n=1}^{+\infty} \frac{a_n}{10^n}. \text{ Then } f \text{ doesn't glue together elements of } \Omega.$$

After the **[PART 1]** and **[PART 2]** we can say that f is one-to-one mapping $\Omega \rightarrow (0,1)$.

For every allowable sequence d_1, d_2, d_3, \dots the mapping f compares the unique real number

$P \in (0,1)$ such that $P = \sum_{n=1}^{+\infty} \frac{d_n}{10^n}$. From here immediately follows the converse assertion: for any

real number $P \in (0,1)$ there exist the unique allowable sequence d_1, d_2, d_3, \dots such that $P = \sum_{n=1}^{+\infty} \frac{d_n}{10^n}$.

Def. For any real number $P \in (0,1)$, where $P = \sum_{n=1}^{+\infty} \frac{d_n}{10^n}$, the symbol $0, d_1 d_2 d_3, \dots$ is called a decimal notation of P .

Next, for any other real number $a \in R$ ([assertion5](#)) there exist the unique pair of integer numbers $k, k+1$ such that $k \leq a < k+1$. As we proved earlier, any integer number k has a unique decimal notation $k \equiv \pm \partial_1 \partial_2 \dots \partial_n$.

If $a = k$, then the decimal notation $\pm \partial_1 \partial_2 \dots \partial_n$ of k is called a decimal notation of a .

If $a \neq k$, then $k < a < k+1 \Rightarrow a = k + (a-k) \parallel (a-k) \in (0,1)$.

As we showed above, the number $(a-k) \in (0,1)$ can be uniquely represented as a sum of

a special series $(a-k) = \sum_{n=1}^{+\infty} \frac{d_n}{10^n}$, then $a = k + (a-k) \Rightarrow a = k + \sum_{n=1}^{+\infty} \frac{d_n}{10^n}$ and the symbol $\pm \partial_1 \partial_2 \dots \partial_n, d_1 d_2 d_3, \dots$ is called a decimal notation of a .

Exponent

Assertion3. The sequence $\{x_n\} \equiv \left(1 + \frac{1}{n}\right)^n$ converges.

Proof. We will show that $\{x_n\}$ is monotonically increasing and bounded above, from here will follow that $\{x_n\}$ converges.

[A] $\{x_n\}$ monotonically increasing. Let's show that $\frac{x_{n+1}}{x_n} \geq 1 \Leftrightarrow x_{n+1} \geq x_n$ (for any $n \in \mathbb{N}$)

$$\begin{aligned} \frac{x_{n+1}}{x_n} &= \frac{\left(1 + \frac{1}{n+1}\right)^{n+1}}{\left(1 + \frac{1}{n}\right)^n} = \left(1 + \frac{1}{n}\right) \cdot \frac{\left(1 + \frac{1}{n+1}\right)^{n+1}}{\left(1 + \frac{1}{n}\right)^{n+1}} = \left(1 + \frac{1}{n}\right) \cdot \left(\frac{1 + \frac{1}{n+1}}{1 + \frac{1}{n}}\right)^{n+1} = \left(1 + \frac{1}{n}\right) \cdot \left(\frac{n+2}{n+1} \cdot \frac{n+1}{n}\right)^{n+1} = \\ &= \left(1 + \frac{1}{n}\right) \cdot \left(\frac{n^2 + 2n}{(n+1)^2}\right)^{n+1} = \left(1 + \frac{1}{n}\right) \cdot \left(\frac{(n+1)^2 - 1}{(n+1)^2}\right)^{n+1} = \left(1 + \frac{1}{n}\right) \cdot \left(1 - \frac{1}{(n+1)^2}\right)^{n+1} \geq // \text{Bernoulli} // \geq \\ &\geq \left(1 + \frac{1}{n}\right) \cdot \left(1 - (n+1) \frac{1}{(n+1)^2}\right) = \left(1 + \frac{1}{n}\right) \cdot \left(1 - \frac{1}{(n+1)}\right) = \left(1 + \frac{1}{n}\right) \cdot \left(\frac{n}{(n+1)}\right) = 1. \text{ So } \frac{x_{n+1}}{x_n} \geq 1. \end{aligned}$$

[B] In the exactly similar way we can show that the sequence $\{y_n\} \equiv \left(1 - \frac{1}{n}\right)^n \parallel n \geq 2$ is

monotonically increasing. And for any $n \in \mathbb{N}$ we have $x_n \cdot y_n \equiv \left(1 + \frac{1}{n}\right)^n \cdot \left(1 - \frac{1}{n}\right)^n = \left(1 - \frac{1}{n^2}\right)^n \leq 1$,

then $x_n \leq \frac{1}{y_n}$. As $\{y_n\}$ is monotonically increasing, then $y_n \geq y_2 \parallel n \geq 2$, then

$x_n \leq \frac{1}{y_n} \leq \frac{1}{y_2} = 4 \parallel n \geq 2$. Then $\{x_n\}$ is bounded above.

So $\{x_n\} \equiv \left(1 + \frac{1}{n}\right)^n$ converges, the limit of this sequence (the number) is denoted like e and called “an exponent”. Practical calculations show that $e \approx 2,71828$ (the sign \approx means “approximately equal”).

Def. For any natural number $n \in \mathbb{N}$ we define $n! \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$ and also $0! \equiv \text{by def} / \equiv 1$.

Def. For any pair of integers $n \geq k \parallel n \in \mathbb{N}, k \geq 0$ the next number $C_n^k \equiv \frac{n!}{k!(n-k)!}$ is called a binomial coefficient.

Exercise1. For any pair of integers $n \geq k \parallel n \in \mathbb{N}, k \geq 0$, the binomial coefficient $C_n^k \equiv \frac{n!}{k!(n-k)!}$ is a natural number. And C_n^k is a number of different k -element subsets of the set $\{1, 2, 3, \dots, n\}$.

Show that $C_n^0 = 1, C_n^1 = n, C_n^2 = \frac{n(n-1)}{2}, C_n^n = 1$.

Exercise2 (Binomial theorem). For any $a, b \in \mathbb{R}$ any $n \in \mathbb{N}$ the next formula is true

$$(a+b)^n = \sum_{k=0}^n C_n^k \cdot a^k \cdot b^{n-k} = C_n^0 a^0 b^n + C_n^1 a^1 b^{n-1} + C_n^2 a^2 b^{n-2} + \dots + C_n^{n-1} a^{n-1} b^1 + C_n^n a^n.$$

Notice, the **Binomial theorem** can be proved by induction, or by a simple reasoning:

$(a+b)^n = (a+b) \cdot (a+b) \cdot \dots \cdot (a+b)$, we need to understand which summands will appear on the right side after we simplify the expression (after we expand the brackets on the right side).

Assertion4. The series $1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!} + \dots$ **[S]** converges to e . And for any natural

number $n \in \mathbb{N}$ there exist the real number $\theta \in (0,1)$ such that $e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!} + \frac{\theta}{n!n}$.

Proof. We have proved above that the sequence $\{x_n\} \equiv \left(1 + \frac{1}{n}\right)^n$ is monotonically increasing and

goes to e . Let's expand the brackets:

$$\begin{aligned} x_n &= \left(1 + \frac{1}{n}\right)^n = \left(\frac{1}{n} + 1\right)^n = \sum_{k=0}^n C_n^k \frac{1}{n^k} = C_n^0 + C_n^1 \frac{1}{n} + C_n^2 \frac{1}{n^2} + \dots + C_n^{n-1} \frac{1}{n^{n-1}} + C_n^n \frac{1}{n^n} = \\ &= \left(\frac{n!}{0!n!}\right) + \left(\frac{n!}{1!(n-1)!}\right) \cdot \frac{1}{n} + \left(\frac{n!}{2!(n-2)!}\right) \cdot \frac{1}{n^2} + \left(\frac{n!}{3!(n-3)!}\right) \cdot \frac{1}{n^3} + \dots + \left(\frac{n!}{k!(n-k)!}\right) \cdot \frac{1}{n^k} + \dots + \left(\frac{n!}{n!0!}\right) \cdot \frac{1}{n^n} = \\ &= 1 + \left(\frac{n}{1!}\right) \cdot \frac{1}{n} + \left(\frac{n(n-1)}{2!}\right) \cdot \frac{1}{n^2} + \left(\frac{n(n-1)(n-2)}{3!}\right) \cdot \frac{1}{n^3} + \dots + \left(\frac{n(n-1)\dots(n-(k-1))}{k!}\right) \cdot \frac{1}{n^k} + \dots + \left(\frac{n(n-1)\dots(n-(n-1))}{n!}\right) \cdot \frac{1}{n^n} = \\ &= 1 + \frac{1}{1!} + \frac{1}{2!} \left(\frac{n(n-1)}{n^2}\right) + \frac{1}{3!} \left(\frac{n(n-1)(n-2)}{n^3}\right) + \dots + \frac{1}{k!} \left(\frac{n(n-1)\dots(n-(k-1))}{n^k}\right) + \dots + \frac{1}{n!} \left(\frac{n(n-1)\dots(n-(n-1))}{n^n}\right) = \\ &= 1 + \frac{1}{1!} + \frac{1}{2!} \left(1 \cdot \left(1 - \frac{1}{n}\right)\right) + \frac{1}{3!} \left(1 \cdot \left(1 - \frac{1}{n}\right) \cdot \left(1 - \frac{2}{n}\right)\right) + \dots + \frac{1}{k!} \left(1 \cdot \left(1 - \frac{1}{n}\right) \cdot \dots \cdot \left(1 - \frac{k-1}{n}\right)\right) + \dots + \frac{1}{n!} \left(1 \cdot \left(1 - \frac{1}{n}\right) \cdot \dots \cdot \left(1 - \frac{n-1}{n}\right)\right) < \\ &< 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!}. \end{aligned}$$

We have shown that $x_n < S_n \parallel \forall n$ **[1-st result]** where S_n is a partial sum

of the series: $1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!} + \dots$. Let's also show that for any n we have $S_n < e$:

We got the representation **[T]**:

$$\begin{aligned} x_n &= 1 + \frac{1}{1!} + \frac{1}{2!} \left(1 \cdot \left(1 - \frac{1}{n}\right)\right) + \frac{1}{3!} \left(1 \cdot \left(1 - \frac{1}{n}\right) \cdot \left(1 - \frac{2}{n}\right)\right) + \dots + \frac{1}{k!} \left(1 \cdot \left(1 - \frac{1}{n}\right) \cdot \dots \cdot \left(1 - \frac{k-1}{n}\right)\right) + \dots \\ &\dots + \frac{1}{n!} \left(1 \cdot \left(1 - \frac{1}{n}\right) \cdot \dots \cdot \left(1 - \frac{n-1}{n}\right)\right). \end{aligned}$$

Let's fix any $\bar{k} \in \mathbb{N} \parallel \bar{k} \geq 2$. And let's consider all the terms of the sequence $\{x_n\}$ with numbers $n > \bar{k}$. In any term $x_n \parallel n > \bar{k}$ we are interested in the first \bar{k} summands from the representation **[T]**.

$$\begin{aligned} &1 + \frac{1}{1!} + \frac{1}{2!} \left(1 \cdot \left(1 - \frac{1}{n}\right)\right) + \frac{1}{3!} \left(1 \cdot \left(1 - \frac{1}{n}\right) \cdot \left(1 - \frac{2}{n}\right)\right) + \dots + \frac{1}{\bar{k}!} \left(1 \cdot \left(1 - \frac{1}{n}\right) \cdot \dots \cdot \left(1 - \frac{\bar{k}-1}{n}\right)\right) \equiv \\ &\equiv \left[\begin{array}{l} \text{the partial sum} \\ \text{of } x_n \parallel n > \bar{k} \end{array} \right] \equiv \tilde{\Sigma}(x_n) \end{aligned}$$

Notice there are exactly \bar{k} summands in any partial sum $\tilde{\Sigma}(x_n)$ for any $x_n \parallel n > \bar{k}$.

For any concrete $n > \bar{k}$ the sum $\tilde{\Sigma}(x_n)$ is a concrete number, and we have the sequence

$\tilde{\Sigma}(x_{k+1}), \tilde{\Sigma}(x_{k+2}), \tilde{\Sigma}(x_{k+3}), \dots$. Every term in this sequence is represented as a sum of \bar{k} summands,

and it's easy to see that the sequence $\tilde{\Sigma}(x_{k+1}), \tilde{\Sigma}(x_{k+2}), \tilde{\Sigma}(x_{k+3}), \dots$ is a sum of several other sequences:

$$\{\tilde{\Sigma}(x_n)\} \equiv \left\{1 + \frac{1}{1!}\right\} + \left\{\frac{1}{2!}\right\} \cdot \left\{\left(1 - \frac{1}{n}\right)\right\} + \left\{\frac{1}{3!}\right\} \cdot \left\{\left(1 - \frac{1}{n}\right)\right\} \cdot \left\{\left(1 - \frac{2}{n}\right)\right\} \dots + \left\{\frac{1}{\bar{k}!}\right\} \cdot \left\{\left(1 - \frac{1}{n}\right)\right\} \cdot \dots \cdot \left\{\left(1 - \frac{\bar{k}-1}{n}\right)\right\}.$$

Some of these sequences go to 1. Really,

$$\left\{ \left(1 - \frac{1}{n} \right) \right\} \xrightarrow{n \rightarrow +\infty} 1, \quad \left\{ \left(1 - \frac{2}{n} \right) \right\} \xrightarrow{n \rightarrow +\infty} 1 \dots \left\{ \left(1 - \frac{\bar{k}-1}{n} \right) \right\} \xrightarrow{n \rightarrow +\infty} 1.$$

And the other sequences are stationary sequences, like $\left\{ \frac{1}{2!} \right\} = \frac{1}{2!}, \frac{1}{2!}, \frac{1}{2!} \dots, \left\{ \frac{1}{3!} \right\} = \frac{1}{3!}, \frac{1}{3!}, \frac{1}{3!} \dots$

$$\text{Then the sequence } \left\{ \left[\begin{array}{l} \text{the partial sum} \\ \text{of } x_n \parallel n > \bar{k} \end{array} \right] \right\} \equiv \{ \tilde{\Sigma}(x_n) \} \xrightarrow{n \rightarrow +\infty} 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{\bar{k}!} \equiv S_{\bar{k}}$$

(where $S_{\bar{k}}$ is a partial sum of the series **[S]**). So $\{ \tilde{\Sigma}(x_n) \} \xrightarrow{n \rightarrow +\infty} S_{\bar{k}}$. From here immediately follows that if we fix any number $v < S_{\bar{k}}$, then all the terms of sequence $\{ \tilde{\Sigma}(x_n) \}$ are greater than v , starting from some moment. Let's fix $S_{\bar{k}-1} < 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{(\bar{k}-1)!} < S_{\bar{k}}$.

Then there exist some number \bar{n} such that $S_{\bar{k}-1} < \tilde{\Sigma}(x_n) \parallel \forall n > \bar{n}$. Then $S_{\bar{k}-1} < \tilde{\Sigma}(x_n) < x_n \parallel \forall n > \bar{n}$ (because every x_n contains it's partial sum $\tilde{\Sigma}(x_n)$).

Every element x_n , in it's turn, is less than e , then $S_{\bar{k}-1} < e$. We had started above from an arbitrary natural number $\bar{k} \geq 2$ and we showed that $S_{\bar{k}-1} < e$, from here follows that:

$S_n < e \parallel \forall n \in \mathbb{N}$ **[2-nd result]** and it is exactly what we need. From the **[1-st result]** and **[2-nd result]** follows that $x_n < S_n < e \parallel \forall n$, then from the squeeze theorem for sequences, $\{S_n\} \rightarrow e$, it means that the series $1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!} + \dots$ goes to e .

Next. Let's show that for any $n \in \mathbb{N}$ there exist $\theta \in (0,1)$ such that

$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!} + \frac{\theta}{n!n} \parallel \theta \in (0,1)$. The sequence of partial sums $\{S_n\}$ is monotonically increasing and goes to e , then $S_n < e \parallel \forall n$. So,

$$\begin{aligned} 0 < e - S_n &= \left(1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!} + \dots \right) - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!} \right) = \\ &= \frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \frac{1}{(n+3)!} + \dots = \frac{1}{n!} \cdot \left(\frac{1}{(n+1)} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + \dots \right) < \\ &< \frac{1}{n!} \cdot \left(\frac{1}{(n+1)} + \frac{1}{(n+1)^2} + \frac{1}{(n+1)^3} + \dots \right) = \frac{1}{n!} \cdot \frac{1}{(n+1)} \cdot \left(1 + \frac{1}{(n+1)} + \frac{1}{(n+1)^2} + \dots \right) = \left[\begin{array}{l} \text{geometric} \\ \text{series} \end{array} \right] = \end{aligned}$$

$$= \frac{1}{n!} \cdot \frac{1}{(n+1)} \cdot \left(\frac{1}{1 - \frac{1}{(n+1)}} \right) = \frac{1}{n!} \cdot \frac{1}{(n+1)} \cdot \frac{(n+1)}{n} = \frac{1}{n!n}. \text{ We have shown that } 0 < e - S_n < \frac{1}{n!n},$$

then there exist some $\theta \in (0,1)$ such that $e - S_n = \frac{\theta}{n!n}$, everything is proved.

Def. Any number $a \in R$, which does not belong to $Q \subset R$, (it means that a can't be represented as a ratio of some integer numbers) is called an irrational number.

Assertion5. e is an irrational number.

Proof. Let's assume the contrary $e = \frac{m}{n} \parallel m, n \in Z$, we can assume that $n \in N$, if not, then

$$e = \frac{m}{n} = \frac{(-1) \cdot m}{(-1) \cdot n} = \frac{-m}{-n}, \text{ where } -n \text{ is already a natural number. So } e = \frac{m}{n} \parallel m \in Z, n \in N.$$

Let's take the representation of e for this number $n \in N$.

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!} + \frac{\theta}{n!n} \parallel \theta \in (0,1) \Leftrightarrow \frac{m}{n} = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!} + \frac{\theta}{n!n} \parallel \theta \in (0,1).$$

Let's multiply both sides by $n!n$, then

$$m \cdot n! = \left(1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!} \right) \cdot n!n + \theta \Rightarrow \theta = m \cdot n! - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!} \right) \cdot n!n.$$

The expression on the right side is obviously an integer number, but θ on the left side is not an integer, $\theta \in (0,1)$. We have a contradiction, therefore e is an irrational number.

Assertion6. The field of rational numbers Q is not a complete field (Q is incomplete).

Proof. The sequence $\{S_n\} = 1, \left(1 + \frac{1}{1!}\right), \left(1 + \frac{1}{1!} + \frac{1}{2!}\right), \left(1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!}\right) \dots$ is obviously a sequence

of rational numbers, and it has a limit e in the field R . Therefore $\{S_n\}$ is fundamental in R ,

then $\{S_n\}$ is fundamental in $Q \subset R$. Let's assume that Q is a complete field.

Then any fundamental sequence in Q has a limit in Q . In particular, $\{S_n\}$ must converge in Q to some limit $q \in Q$. As R is an Archimedean ordered field, which contains Q (look at the [theorem1](#), page 94), the sequence $\{S_n\} \subset Q$ must also converge in R , and it must converge to exactly the same limit $q \in Q$. But we showed above that $\{S_n\}$ converges to $e \notin Q$ in R , we have a contradiction.

Then Q is not a complete field.

8

Construction of Length and Area

Length construction

We must start from the elementary objects: a point, a segment, a line. These are our basic objects. We also make several simple assumptions that are listed below.

We assume that: for any **different** points A, B there exist only one segment AB .

We agree that we understand the phrase:

“The point C lies between A and B ”

[pict1].

Also, any segment AB can be **laid along** any other segment CD [pict2].

Note, when AB is laid along CD , points A and C must coincide.

Suppose we laid AB along CD and:

[A] Points B, D coincide. Then we say

“ AB is equal to CD ”

and we write $AB = CD$.

[B] D is between A and B .

Then we write: $CD < AB$ and

we say “ AB is greater than CD ”, or “ CD is less than AB ”.

[C] B is between A and D . Then we write: $CD > AB$ and we say “ CD is greater than AB ”, or “ AB is less than CD ”. The segment equality “=” is reflexive, symmetric and transitive on Ω , where Ω is the collection of all segments in the space. The relation “<” is transitive on Ω .

Mid-point assumption. For any segment AB there exist the point C such that $AC = CB$.

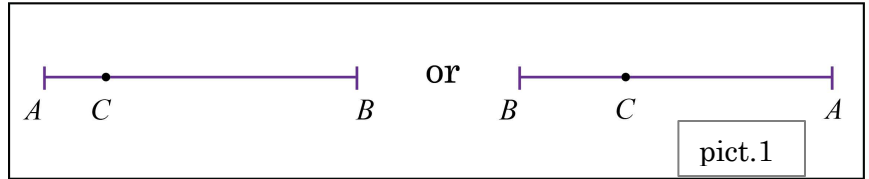
The sum of any segments AB and CD is the segment AD [pict3].

And we write $AD = AB + CD$.

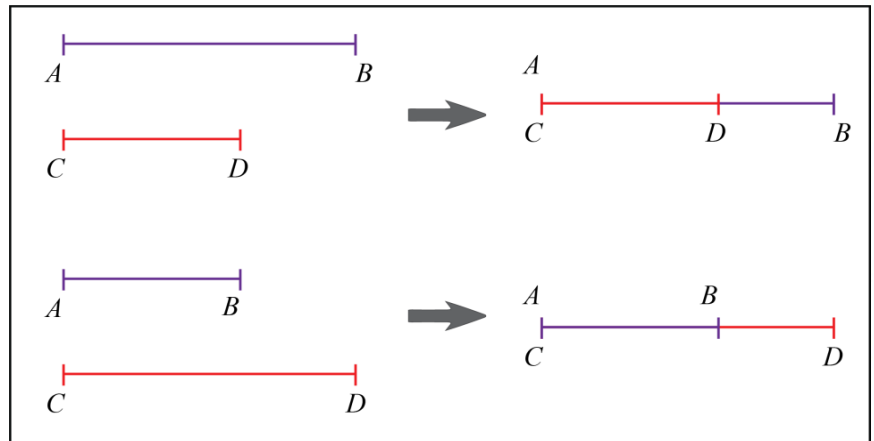
For any natural number n and any

segment AB : the segment nAB is

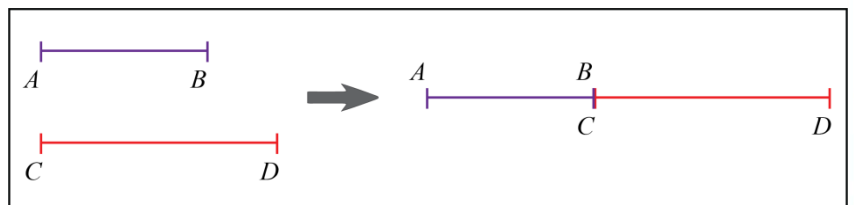
defined like $nAB \equiv AB + AB + \dots + AB$ (there are exactly n “summands” on the right side) [pict4].



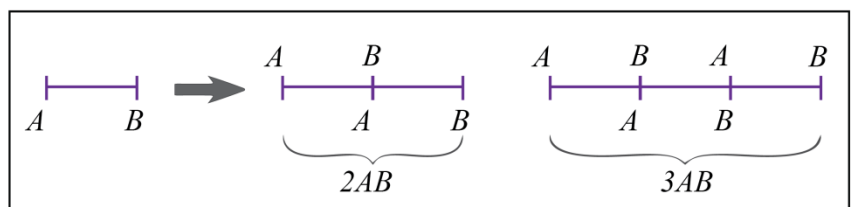
pict.1



pict.2



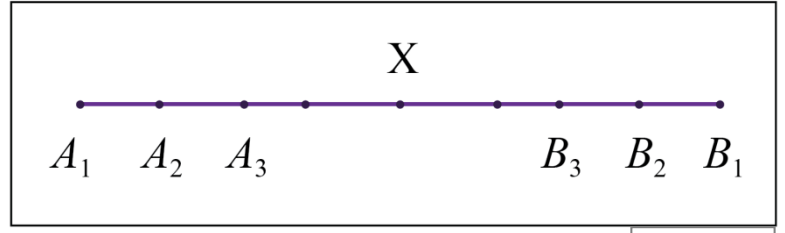
pict.3



pict.4

We also assume that the **Archimedes axiom** is true in Ω : for any segments AB and CD there exist the natural number n such that $nAB > CD$.

And finally, the **axiom of nested segments** is true [pict4.1]: for any sequence of nested segments $A_1B_1 \supset A_2B_2 \supset A_3B_3 \supset \dots$ there exist at least one point X which belongs to every segment: $X \in A_kB_k \ \forall k$.



pict.4.1

This is it, **we have finished with our assumptions.**

Def. If $nAB = CD$ then we say: “ CD is n times greater than AB ” and

“ AB is n times less than CD ” we can also rewrite: $nAB = CD \Leftrightarrow AB \equiv [by\ def] \equiv \frac{CD}{n}$.

From here the next question appears: CD is any segment. For which natural numbers n does the segment $\frac{CD}{n}$ exist? (based on our assumptions). According to the **mid-point assumption**,

the segment $\frac{CD}{n}$ exists for $n = 2$, by using the **mid-point assumption** for the segment $\frac{CD}{2}$ we will

get the segment $\frac{CD}{4}$ and etc. Finally, for any $n = 2^p$ the segment $\frac{CD}{2^p}$ does exist.

At this moment we can't claim that $\frac{CD}{n}$ exists for any natural n , only for n which is a power of 2.

Auxiliary1. For any segments AB and CD there exist the **minimal** natural number p such that:

$$\frac{CD}{2^p} \leq AB.$$

Comment: as p is the minimal natural number with such property, then $\frac{CD}{2^p} \leq AB < \frac{CD}{2^{p-1}}$.

Proof. Let's fix any AB and CD , according to the **Archimedes axiom**, there exist n such that $nAB > CD$. There exist $2^p \geq n$, then $2^p AB \geq nAB$ and therefore $2^p AB \geq CD$ [T].

Let's consider the segment $\frac{CD}{2^p}$, there must be $\frac{CD}{2^p} \leq AB$. Really, if $\frac{CD}{2^p} \geq AB$, then

$$2^p \cdot \left(\frac{CD}{2^p} \right) \geq 2^p \cdot AB \Leftrightarrow CD \geq 2^p \cdot AB \text{ - it contradicts to [T]. So } \frac{CD}{2^p} \leq AB. \text{ From here follows}$$

that the set of natural numbers $\left\{ m \in \mathbb{N} \parallel \frac{CD}{2^m} \leq AB \right\}$ is not empty, then it contains the minimal number p , and p is exactly the number we need.

Length. Ω is a collection of all segments (in the space). The length L is the correspondence $L: \Omega \rightarrow \mathbb{R}^+$. For every concrete segment $\alpha \in \Omega$ a unique positive real number $L(\alpha)$ is defined, $L(\alpha)$ is called a length of α . And $L: \Omega \rightarrow \mathbb{R}^+$ has the next properties:

[1] There exist the segment e such that $L(e) = 1$ (e is called “a scale”).

[2] If $\alpha = \beta$, then $L(\alpha) = L(\beta)$.

[3] $L(\alpha + \beta) = L(\alpha) + L(\beta)$ for any segments α, β .

We will show:

[A] **[Existence]**. If the scale (the segment e) is chosen, the correspondence $L: \Omega \rightarrow \mathbb{R}^+$, such that [1],[2],[3] exists.

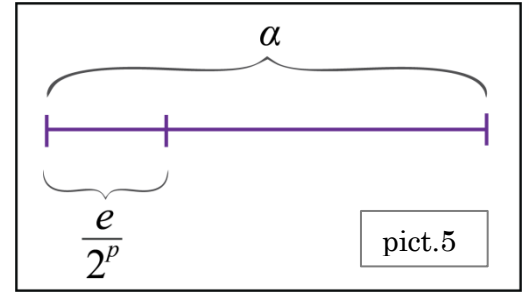
[B] **[Uniqueness]**. If the scale e is fixed, then such correspondence L is unique.

[A] Let's take and fix an arbitrary segment e which we take as a scale. We must define L on every segment. At first we define $L(e) \equiv 1$. Let's fix an arbitrary segment α , the number $L(\alpha)$ is defined as a result of the next process.

The process. [step1] For the pair of segments α, e we take

the minimal natural p such that $\frac{e}{2^p} \leq \alpha$ (**auxiliary1**) the

segment $\frac{e}{2^p}$ can be laid along α at least once [pict5].



Then, according to the **Archimedes axiom**, we can find the natural number T_0 such that:

$$T_0 \left(\frac{e}{2^p} \right) \leq \alpha < (T_0 + 1) \left(\frac{e}{2^p} \right) \text{ [Y1].}$$

So, T_0 is such number that the segment $\frac{e}{2^p}$ can be

placed in α maximum T_0 times, but $(T_0 + 1)$

segments $\frac{e}{2^p}$ already fully cover the segment α

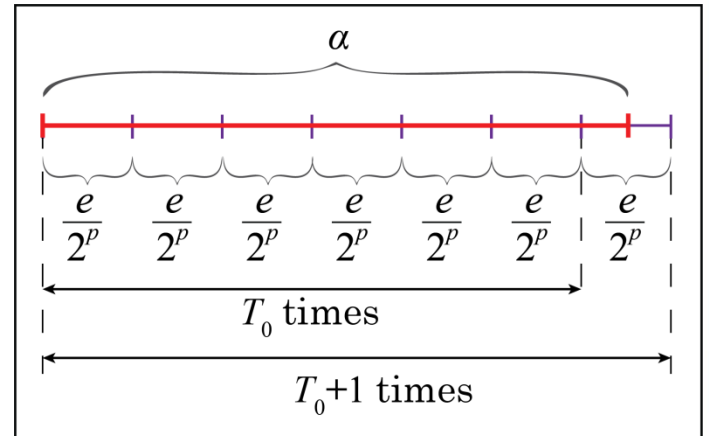
[pict6]. And $(T_0 + 1)$ is a minimal number of

segments $\frac{e}{2^p}$ that we need to cover the segment α

completely. Let's fix the pair of (rational) numbers

$\frac{T_0}{2^p}$ and $\frac{T_0 + 1}{2^p}$. (we had started here from the

segment $\frac{e}{2^p}$, and we got two fractions with denominators 2^p).



pict.6

[step2] We consider the segment $\frac{e}{2^{p+1}}$ (which is a half of the initial segment $\frac{e}{2^p}$) and we perform the **[step1]** for the segments $\frac{e}{2^{p+1}}$ and α . So, there exist the natural T_1 such that

$$T_1 \left(\frac{e}{2^{p+1}} \right) \leq \alpha < (T_1 + 1) \left(\frac{e}{2^{p+1}} \right) \text{ [Y2].}$$

Let's show that **[A]** $2T_0 \leq T_1$ and **[B]** $T_1 + 1 \leq 2(T_0 + 1)$. The segment $\frac{e}{2^p}$ can be placed in α exactly T_0 times, every segment $\frac{e}{2^p}$ contains exactly two segments $\frac{e}{2^{p+1}}$, then α contains (for sure) $2T_0$ segments $\frac{e}{2^{p+1}}$. But T_1 is a maximal number of segments $\frac{e}{2^{p+1}}$ which we can place in α , then $2T_0 \leq T_1$ (**[A]** is done).

Next, $T_0 + 1$ segments $\frac{e}{2^p}$ cover α completely, each segment $\frac{e}{2^p}$ contains exactly two segments $\frac{e}{2^{p+1}}$, then $2(T_0 + 1)$ segments $\frac{e}{2^{p+1}}$ cover α completely. But $T_1 + 1$ is a minimal number of segments $\frac{e}{2^{p+1}}$ that we need to cover the segment α , then $T_1 + 1 \leq 2(T_0 + 1)$ (**[B]** is done).

Let's divide both inequalities **[A]** and **[B]** by 2^{p+1} , then $\frac{T_0}{2^p} \leq \frac{T_1}{2^{p+1}}$ and $\frac{T_1 + 1}{2^{p+1}} \leq \frac{T_0 + 1}{2^p}$ **[E]**.

(we had started here from the segment $\frac{e}{2^{p+1}}$, and we got two new fractions with denominators 2^{p+1})

Next, we take the segment $\frac{e}{2^{p+2}}$ (which is a half of the previous one $\frac{e}{2^{p+1}}$). And we perform the **[step1]** for $\frac{e}{2^{p+2}}, \alpha$. We will find the number T_2 such that $T_2 \left(\frac{e}{2^{p+2}} \right) \leq \alpha < (T_2 + 1) \left(\frac{e}{2^{p+2}} \right)$.

By the similar reasoning we deduce that $2T_1 \leq T_2$ and $T_2 + 1 \leq 2(T_1 + 1)$, we divide these inequalities by 2^{p+2} , then we get $\frac{T_1}{2^{p+1}} \leq \frac{T_2}{2^{p+2}}$ and $\frac{T_2 + 1}{2^{p+2}} \leq \frac{T_1 + 1}{2^{p+1}}$. (we had started here from the segment $\frac{e}{2^{p+2}}$, and we got two new fractions with denominators 2^{p+2}).

Let's compare it with **[E]**, so $\frac{T_0}{2^p} \leq \frac{T_1}{2^{p+1}} \leq \frac{T_2}{2^{p+2}}$ and $\frac{T_2 + 1}{2^{p+2}} \leq \frac{T_1 + 1}{2^{p+1}} \leq \frac{T_0 + 1}{2^p}$.

Now we take the segment $\frac{e}{2^{p+3}}$ (which is a half of the previous one $\frac{e}{2^{p+2}}$). And we make the **[step1]** for $\frac{e}{2^{p+3}}, \alpha$ and etc.

As a result we get the pair of sequences $\frac{T_0}{2^p} \leq \frac{T_1}{2^{p+1}} \leq \frac{T_2}{2^{p+2}} \leq \dots \leq \frac{T_2+1}{2^{p+2}} \leq \frac{T_1+1}{2^{p+1}} \leq \frac{T_0+1}{2^p}$.

Let's show that both sequences $\left\{ \frac{T_k}{2^{p+k}} \right\}, \left\{ \frac{T_k+1}{2^{p+k}} \right\} k = 0, 1, 2 \dots$ converge to the same limit.

It's easy to see that $\left\{ \frac{T_k}{2^{p+k}} \right\}$ is monotonically increasing and bounded above (by $\frac{T_0+1}{2^p}$ for example)

then, according to the theorem about a limit of a monotonic sequence, $\left\{ \frac{T_k}{2^{p+k}} \right\}$ converges to some

limit A . Similarly, the second sequence $\left\{ \frac{T_k+1}{2^{p+k}} \right\}$ is monotonically decreasing and bounded below

(by $\frac{T_0}{2^p}$ for example), then it converges to some limit B . As the difference of the sequences $\left\{ \frac{T_k+1}{2^{p+k}} \right\}$

and $\left\{ \frac{T_k}{2^{p+k}} \right\}$ is an infinitely small sequence $\left\{ \frac{1}{2^{p+k}} \right\} k = 0, 1, 2 \dots$, there must be $A = B$.

Let's sum up. We had started from an arbitrary segment α and we described the concrete process which always gives only one concrete real number $A = B$, then we define: $L(\alpha) \equiv A = B$, i.e., the length of the segment α is a common limit of our sequences.

Comment: during the construction process there was a phrase "we will find", because people usually understand the process better in such formulation. But normally, there must be the phrase "there exist" instead of it, it is more rigorous. Of course, no one really assumes that some person will repeat "by hand" the **[step1]** again and again for pairs of segments, it is virtually impossible. Anyway, we need only the fact of existence of such sequences with a common limit, and we have it now. Some people may be puzzled, because there is an "infinite process", so there are infinitely many steps, and if we make a computer program with such algorithm, it will never stop working. But it is a great process, according to mathematics. The similar processes are embedded in the fundamental theorems of analysis, differential equations, linear algebra, abstract algebra and etc.

We just need to remember that mathematics is not programming, the greatest theorems in mathematics are the theorems that prove the facts of existence of some value/solution/figure and etc. And if we want to make a computer program, we will write a program with a needed process and we will repeat it many times, in order to get a very good approximation of the value we need.

Ok, now L is defined on every segment $\alpha \in \Omega$. Let's show that L satisfies the requirements **[1],[2],[3]** (from the initial definition). **[2]** is obvious. Really, let $\alpha = \beta$, then we lay α along β and they coincide. Then we perform the process, which is described above, for the segment α , in the same time it is the process for the segment β , so on the one hand we will get the length $L(\alpha)$, and on the other hand we will get $L(\beta)$. And $L(\alpha) = L(\beta)$.

Let's show that $L(e) = 1$ (it is [1]). We must perform the process, which is described above, for

the segment e . At first we need to find the minimal p such that $\frac{e}{2^p} \leq e$. Obviously $p = 1$,

because $\frac{e}{2} < e$, then we will get $T_0 = 2, T_1 = 4, T_2 = 8 \dots T_k = 2^{1+k}$. And we have two sequences

$$\frac{2}{2^1} \leq \frac{4}{2^{1+1}} \leq \frac{8}{2^{1+2}} \leq \dots \leq \frac{8+1}{2^{1+2}} \leq \frac{4+1}{2^{1+1}} \leq \frac{2+1}{2^1}$$
 both these sequences converge to 1, then $L(e) = 1$.

Let's finally show that $L(\alpha + \beta) = L(\alpha) + L(\beta)$ (which is [3]). We fix arbitrary segments α, β .

Let's add these segments: $\alpha + \beta = \gamma$.

For each segment α, β, γ we will build it's own sequence (to determine it's length).

$$\text{For } \alpha \text{ we build } \frac{T_0}{2^p} \leq \frac{T_1}{2^{p+1}} \leq \frac{T_2}{2^{p+2}} \leq \dots \leq \frac{T_2+1}{2^{p+2}} \leq \frac{T_1+1}{2^{p+1}} \leq \frac{T_0+1}{2^p}.$$

$$\text{For } \beta \text{ we build } \frac{M_0}{2^d} \leq \frac{M_1}{2^{d+1}} \leq \frac{M_2}{2^{d+2}} \leq \dots \leq \frac{M_2+1}{2^{d+2}} \leq \frac{M_1+1}{2^{d+1}} \leq \frac{M_0+1}{2^d}.$$

$$\text{And for } \gamma \text{ we build } \frac{S_0}{2^m} \leq \frac{S_1}{2^{m+1}} \leq \frac{S_2}{2^{m+2}} \leq \dots \leq \frac{S_2+1}{2^{m+2}} \leq \frac{S_1+1}{2^{m+1}} \leq \frac{S_0+1}{2^m}.$$

Let's take $h \equiv \max(p, d, m)$, we want to have the sequences which all start from the fractions with the same denominators 2^h , so we can discard several initial terms in each sequence, it does not affect convergence and the limit value. There is no need to complicate our designations, and we can assume that all our sequences (from the very beginning) start from the fractions with the same denominators 2^h .

$$\text{For } \alpha : \frac{T_0}{2^h} \leq \frac{T_1}{2^{h+1}} \leq \frac{T_2}{2^{h+2}} \leq \dots \leq \frac{T_2+1}{2^{h+2}} \leq \frac{T_1+1}{2^{h+1}} \leq \frac{T_0+1}{2^h}.$$

$$\text{For } \beta : \frac{M_0}{2^h} \leq \frac{M_1}{2^{h+1}} \leq \frac{M_2}{2^{h+2}} \leq \dots \leq \frac{M_2+1}{2^{h+2}} \leq \frac{M_1+1}{2^{h+1}} \leq \frac{M_0+1}{2^h} \quad [\text{V}].$$

$$\text{For } \gamma : \frac{S_0}{2^h} \leq \frac{S_1}{2^{h+1}} \leq \frac{S_2}{2^{h+2}} \leq \dots \leq \frac{S_2+1}{2^{h+2}} \leq \frac{S_1+1}{2^{h+1}} \leq \frac{S_0+1}{2^h}.$$

Let's remember the meaning of these numbers. So, T_0 segments $\frac{e}{2^h}$ can be placed in the segment

α , and M_0 segments $\frac{e}{2^h}$ can be placed in the segment β , so with guarantee $T_0 + M_0$ segments $\frac{e}{2^h}$

can be placed in the segment $\alpha + \beta$ (and maybe more). And S_0 is a maximal number of segments

$\frac{e}{2^h}$, which we can place in $\gamma = \alpha + \beta$, then $T_0 + M_0 \leq S_0$. And in the exactly similar way we can

deduce $L_n + M_n \leq S_n$ (for every number n).

Next, $T_0 + 1$ segments $\frac{e}{2^h}$ cover the segment α completely, and $M_0 + 1$ segments $\frac{e}{2^h}$ cover the segment β completely. Then $(T_0 + 1) + (M_0 + 1)$ segments $\frac{e}{2^h}$ (with guarantee) cover the segment $\alpha + \beta$. Let's remember that $S_0 + 1$ is a minimal number of segments $\frac{e}{2^h}$ that we need to cover the segment $\gamma = \alpha + \beta$, then $S_0 + 1 \leq (T_0 + 1) + (M_0 + 1)$. And similarly we get: $S_n + 1 \leq (T_n + 1) + (M_n + 1) \quad \forall n$. So we have:

$$\forall n \parallel \begin{array}{l} T_n + M_n \leq S_n \\ S_n + 1 \leq (T_n + 1) + (M_n + 1) \end{array} \Rightarrow \begin{array}{l} T_n + M_n \leq S_n \\ S_n \leq T_n + M_n + 1 \end{array} \Rightarrow L_n + M_n \leq S_n \leq L_n + M_n + 1,$$

let's divide all the sides by 2^{h+n} , then: $\frac{T_n}{2^{h+n}} + \frac{M_n}{2^{h+n}} \leq \frac{S_n}{2^{h+n}} \leq \frac{T_n}{2^{h+n}} + \frac{M_n}{2^{h+n}} + \frac{1}{2^{h+n}}$.

Let's use the squeeze theorem for sequences (look at **[V]**):

$$\left\{ \frac{T_n}{2^{h+n}} \right\} + \left\{ \frac{M_n}{2^{h+n}} \right\} \xrightarrow{n \rightarrow \infty} L(\alpha) + L(\beta) \text{ and } \left\{ \frac{T_n}{2^{h+n}} \right\} + \left\{ \frac{M_n}{2^{h+n}} \right\} + \left\{ \frac{1}{2^{h+n}} \right\} \xrightarrow{n \rightarrow \infty} L(\alpha) + L(\beta) + 0,$$

then there must be $\left\{ \frac{S_n}{2^{h+n}} \right\} \rightarrow L(\alpha) + L(\beta)$. And we already have **[V]** $\left\{ \frac{S_n}{2^{h+n}} \right\} \rightarrow L(\gamma)$.

Then $L(\alpha) + L(\beta) = L(\gamma) = L(\alpha + \beta)$, everything is proved.

We have proved the existence of the length. Let's prove the uniqueness.

Let L is any correspondence $\Omega \rightarrow R^+$ such that **[1],[2],[3]**, so L is not necessary the same correspondence as we built above.

[Property1]. From **[3]** follows that for any segments $\alpha_1, \dots, \alpha_n$ we have

$$L(\alpha_1 + \dots + \alpha_n) = L(\alpha_1) + \dots + L(\alpha_n), \text{ and in particular}$$

$$L(n\alpha) = L(\alpha + \dots + \alpha) = L(\alpha) + \dots + L(\alpha) = n \cdot L(\alpha).$$

From here follows that for any number 2^{p+k} we have $L\left(\frac{e}{2^{p+k}}\right) = \frac{1}{2^{p+k}}$, really

$$\frac{e}{2^{p+k}} + \dots + \frac{e}{2^{p+k}} = [2^{p+k} \text{ summands}] = e, \text{ then}$$

$$L\left(\frac{e}{2^{p+k}} + \dots + \frac{e}{2^{p+k}}\right) = L(e) \Rightarrow L\left(\frac{e}{2^{p+k}}\right) + \dots + L\left(\frac{e}{2^{p+k}}\right) = 1 \Rightarrow L\left(\frac{e}{2^{p+k}}\right) \cdot 2^{p+k} = 1 \Rightarrow L\left(\frac{e}{2^{p+k}}\right) = \frac{1}{2^{p+k}}.$$

[Property2]. For any segments α, β we have $\alpha > \beta \Leftrightarrow L(\alpha) > L(\beta)$.

Really, let $\alpha > \beta \Leftrightarrow \alpha = \beta + \delta$ where δ is some segment, then $L(\alpha) = L(\beta) + L(\delta) \Rightarrow L(\alpha) > L(\beta)$.

Conversely, let $L(\alpha) > L(\beta)$. There are exactly three variants: $\alpha = \beta$, $\beta > \alpha$, $\alpha > \beta$.

If $\alpha = \beta$, then $L(\alpha) = L(\beta)$, which is not true. If $\beta > \alpha$, then $L(\beta) > L(\alpha)$, which is not true. So, the last possibility is $\alpha > \beta$. Everything is proved.

Uniqueness. Let \tilde{L} is some other “length” (the correspondence $\Omega \rightarrow R^+$ such that [1],[2],[3]). From [1] we have $\tilde{L}(e) = L(e)$. Let’s fix an arbitrary segment α . And let’s build two sequences as above $\frac{T_0}{2^p} \leq \frac{T_1}{2^{p+1}} \leq \frac{T_2}{2^{p+2}} \leq \dots \leq \frac{T_2+1}{2^{p+2}} \leq \frac{T_1+1}{2^{p+1}} \leq \frac{T_0+1}{2^p}$. According to the process, which is described above, for any $k = 0, 1, 2, 3, \dots$ we have $T_k \left(\frac{e}{2^{p+k}} \right) \leq \alpha < (T_k + 1) \left(\frac{e}{2^{p+k}} \right)$. Then for \tilde{L} ([property2]) we have $\tilde{L} \left(T_k \left(\frac{e}{2^{p+k}} \right) \right) \leq \tilde{L}(\alpha) < \tilde{L} \left((T_k + 1) \left(\frac{e}{2^{p+k}} \right) \right) \Rightarrow T_k \cdot \tilde{L} \left(\frac{e}{2^{p+k}} \right) \leq \tilde{L}(\alpha) < (T_k + 1) \cdot \tilde{L} \left(\frac{e}{2^{p+k}} \right) \Rightarrow$ ([property1]) $T_k \cdot \frac{1}{2^{p+k}} \leq \tilde{L}(\alpha) < (T_k + 1) \cdot \frac{1}{2^{p+k}} \Leftrightarrow \frac{T_k}{2^{p+k}} \leq \tilde{L}(\alpha) < \frac{T_k + 1}{2^{p+k}}$. Both sequences $\left\{ \frac{T_k}{2^{p+k}} \right\}$ and $\left\{ \frac{T_k + 1}{2^{p+k}} \right\}$ converge to $L(\alpha)$ (by definition, we have defined $L(\alpha)$ as a common limit of these sequences). Then from $\frac{T_k}{2^{p+k}} \leq \tilde{L}(\alpha) < \frac{T_k + 1}{2^{p+k}}$ (squeeze theorem for sequences) we get $\tilde{L}(\alpha) = L(\alpha)$. Then the values $L(\alpha)$ and $\tilde{L}(\alpha)$ are equal on every segment α , then $\tilde{L} \equiv L$.

Let’s resolve now the question about the existence of the segment $\frac{\alpha}{n}$ (where α is some segment and n is a natural number). Now we know only that $\frac{\alpha}{n}$ exists when n is a power of two: $n = 2^p$.

We need to prove the next property.

[Property3]. For any positive real number a there exist some segment α such that $L(\alpha) = a$.

Proof. Let’s remember the chapter “Pre-real numbers” there was an [Example L] (page 94), in which we had taken an arbitrary positive element a (which belonged to some Archimedean ordered field which contained Q , and now $a \in R \supset Q$). We had fixed any $n \in \mathbb{N}$ such that $\frac{1}{n} \leq a$, and then we

built the rational sequence $\left\{ \frac{T_k}{2^k n} \right\} \parallel k = 0, 1, 2, \dots$ such that

$$\frac{T_0}{n} \leq \frac{T_1}{2n} \leq \frac{T_2}{2^2 n} \leq \frac{T_3}{2^3 n} \leq \dots \leq a < \dots \leq \frac{T_3+1}{2^3 n} \leq \frac{T_2+1}{2^2 n} \leq \frac{T_1+1}{2n} \leq \frac{T_0+1}{n}. \text{ And } \left\{ \frac{T_k}{2^k n} \right\} \rightarrow a.$$

Let’s notice that the difference of the sequences $\left\{ \frac{T_k+1}{2^k n} \right\}, \left\{ \frac{T_k}{2^k n} \right\}$ is an infinitely small sequence

$$\left\{ \frac{1}{2^k n} \right\}, \text{ and therefore we also have } \left\{ \frac{T_p+1}{2^p n} \right\} \rightarrow a.$$

Let's fix now any positive real number $a \in R$, we can find the minimal natural number p such that

$\frac{1}{2^p} \leq a$. Let's take then $n \equiv 2^p$ and build two sequences (from the [\[Example L\]](#)).

So we have $\frac{T_0}{2^p} \leq \frac{T_1}{2^{p+1}} \leq \frac{T_2}{2^{p+2}} \leq \frac{T_3}{2^{p+3}} \leq \dots \leq a < \dots \leq \frac{T_3+1}{2^{p+3}} \leq \frac{T_2+1}{2^{p+2}} \leq \frac{T_1+1}{2^{p+1}} \leq \frac{T_0+1}{2^p}$ [S].

Let's take now the scale segment e , we know that for any $k \in \mathbb{N}$ the segment $\frac{e}{2^{p+k}}$ exists, then

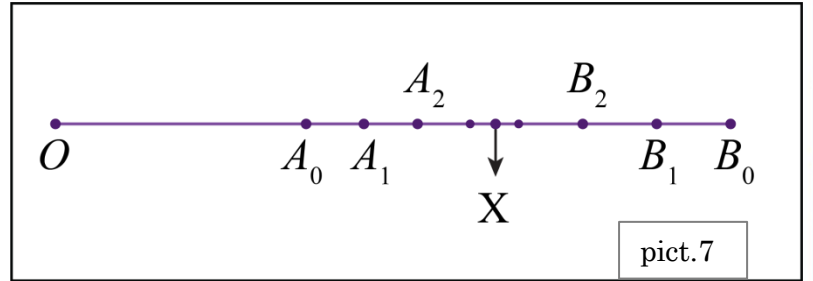
for any natural number T_k the segment $T_k \cdot \frac{e}{2^{p+k}}$ also exists.

Let's use the sequences [S] in order to build the sequence of nested segments. We fix any point O , and build the segment $OA_0 = T_0 \cdot \frac{e}{2^p}$, then we lay the segment $OB_0 = (T_0 + 1) \cdot \frac{e}{2^p}$ along OA_1 .

Then we build $OA_1 = T_1 \cdot \frac{e}{2^{p+1}}$ and

$OB_1 = (T_1 + 1) \cdot \frac{e}{2^{p+1}}$ [pict7], then

$OA_2 = T_2 \cdot \frac{e}{2^{p+2}}$ and $OB_2 = (T_2 + 1) \cdot \frac{e}{2^{p+2}}$



and etc. The segments $A_0B_0, A_1B_1, A_2B_2 \dots$ are obviously the nested segments, then (according to the **axiom of nested segments**) there exist some point X which belongs to every segment.

This point is unique, because the length $L(A_kB_k) = \frac{1}{2^{p+k}}$, and if we assume that there also exists some other point Y which belongs to every segment, then every segment A_kB_k contains the segment XY , then $L(A_kB_k) \geq L(XY) = \text{const} \forall k$ which contradicts to $L(A_kB_k) = \frac{1}{2^{p+k}} \xrightarrow{k \rightarrow \infty} 0$.

Then the segment OX is exactly the segment, for which $L(OX) = a$. Really, according to our construction process we have: $L(OA_k) \leq L(OX) \leq L(OB_k) \parallel \forall k$ and $L(OA_k) = L\left(T_k \cdot \frac{e}{2^{p+k}}\right) = \frac{T_k}{2^{p+k}}$

and $L(OB_k) = L\left((T_k + 1) \cdot \frac{e}{2^{p+k}}\right) = \frac{(T_k + 1)}{2^{p+k}}$, then $\frac{T_k}{2^{p+k}} \leq L(OX) \leq \frac{(T_k + 1)}{2^{p+k}} \parallel \forall k$ [F] and both

sequences $\left\{ \frac{T_k}{2^{p+k}} \right\}$ and $\left\{ \frac{T_k + 1}{2^{p+k}} \right\}$ converge to the number a (these sequences are built in such way).

Then from [F] and from the **squeeze theorem for sequences** follows that $L(OX) = a$.

Let's fix now an arbitrary segment α and any natural number n . Let's take the positive real number $\frac{L(\alpha)}{n}$. According to the [\[property3\]](#), there exist the segment β which's length is

$L(\beta) = \frac{L(\alpha)}{n}$. Let's show that if we lay β along α exactly n times we will get the segment $n\beta$

which coincides with α (then $n\beta = \alpha$ and then $\beta = \frac{\alpha}{n}$ by definition).

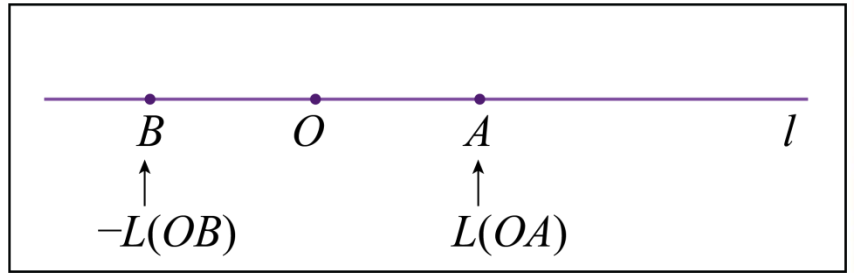
Let's lay the segment β exactly n times along α , we will get segment $n\beta$ which is laid along α . If $n\beta$ coincides with α , then everything is proved. Suppose that $n\beta$ does not coincide with α . Then there can be exactly two variants: **[First]** $n\beta > \alpha$, then **[property2]** we have $L(n\beta) > L(\alpha) \Rightarrow$ **[property1]** $\Rightarrow L(\beta) + \dots + L(\beta) > L(\alpha) \Leftrightarrow \frac{L(\alpha)}{n} + \dots + \frac{L(\alpha)}{n} > L(\alpha) \Leftrightarrow L(\alpha) > L(\alpha)$ and we have a contradiction.

[Second] $n\beta < \alpha$, we will get here a similar contradiction (as we got in the first case). Then $n\beta$ must coincide with α and everything is proved.

Note. In practice, for convenience, we do not write the letter L to denote a length of a segment. Instead of $L(\alpha) = 5$ we write just $\alpha = 5$. Instead of $L(AB) = 10$ we write just $AB = 10$.

Line coordinates. **[pict8]** Let's fix any line l , we mark any point O on this line, the point O divides the line in two rays, we compare the real number zero 0 to the point O .

We need to choose any segment e as a scale, so $e \equiv 1$. Then we choose one of two rays (any one), we will call it "a positive ray". For any point $A \neq O$ on the positive ray we compare a positive real number: a length of a segment OA .



The other ray is called "a negative ray".

And for any point $B \neq O$ on the negative

ray we compare a negative real number: a length of a segment OB with the minus sign $-OB$.

pict.8

Def. For any point A on l , the real number a , which is compared to A , is called a coordinate of A . And l is called a coordinate line.

We have defined the mapping $f: l \rightarrow R$. Let's show that this mapping is one-to-one.

At first, it covers R . Really, it's very easy to show by using the **[property3]**: for any positive real number a there exist some segment α such that $L(\alpha) = a$. Secondly, we need to show that $f: l \rightarrow R$ doesn't "glue together" points of l , i.e., if $A \neq B$ are different points, then numbers $f(A), f(B)$ are also different. It's very easy to show just by considering all the possible cases:

[A] some point A or B coincides with O , and the other lies on the positive/negative ray.

[B] none of A, B coincide with O , then there may be: both A, B are on the positive ray, both on the negative ray, one point on the positive ray and the other one on the negative ray.

In each case it's very easy to understand that $f(A), f(B)$ are different real numbers.

Then $f : l \rightarrow R$ is one-to-one. From here follows that the inverse mapping $f^{-1} : R \rightarrow l$ is also one-to-one, describe this mapping.

Let's sum up: for every line l there exist one-to-one correspondence (the mapping) $\varphi : R \rightarrow l$.

Because of that we say that a coordinate line l is a “geometrical interpretation”, or a “visual interpretation” of real numbers. A visual interpretation l of real numbers has some amazing properties which can simplify our actions (with real numbers). For example, for any $a \in R$ the absolute value $|a| = L(OA)$ (where A is the point on l with a coordinate a). Also, for any real numbers a, b , the number $|a - b|$ is a length of the segment AB , where A and B are the points on l with coordinates a and b .

Also, $a < b < c$ if and only if B lies between A and C . When we add positive numbers we can represent it as we take one segment and put it next to the other segment. Addition of negative numbers has a similar representation.

Any segment $[a, b]$ /interval (a, b) /half-interval $(a, b]$ or $[a, b)$ of real numbers has a visual interpretation as a segment AB /interval (AB) /half-interval $(AB]$ or $[A, B)$ on the line.

Any ε -neighborhood $O_\varepsilon(a)$ of a real number a has a visual interpretation as an interval with the center at A .

So, the use of a visual representation is a very handy tool, it may help us to simplify our reasonings.

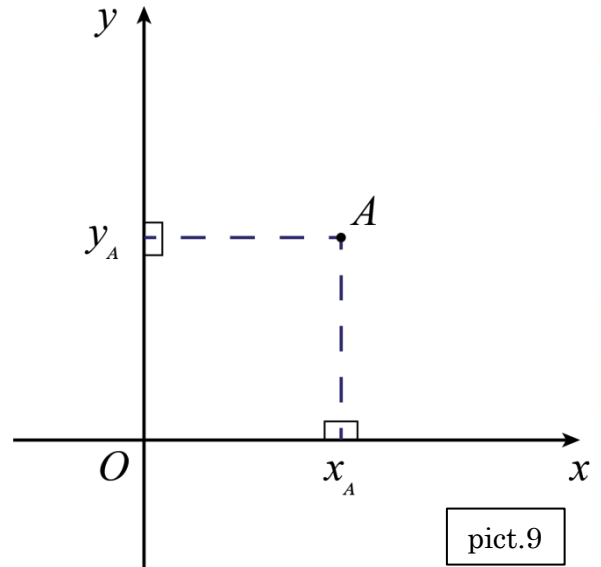
But it's important to remember that when we perform actions like addition/subtraction/multiplication/division of real numbers we “work” inside the field R , and we do it by the rules of R , these rules are precisely defined on R , and they don't have any connection with any line.

Many properties of real numbers do not have any visual interpretation, the field R is an independent structure which consists of numbers (which are symbols), and R includes precise rules, how to operate with all these symbols. In fact, every number is just an abstract symbol, the symbol from R . The connection between real numbers and points is **extremely** important. Plane coordinates and space coordinates allow us to take purely geometrical questions and narrow them down to the questions, concerning real numbers. By using the connection between points and numbers we can precisely describe shapes of objects and their motions. Moreover, there is no other way to describe precisely most of shapes and motions without the use of real numbers.

But the set R of real numbers is a purely abstract (imaginary) set. And we use this set as an auxiliary tool for a huge variety of different purposes. We use real numbers to specify time and dates, to estimate the distance we need to walk and the duration of our journey, to determine our income, our age, how many calories we eat a day, to measure our weight and height, to estimate our lifespan and etc.

But once again, the set of real numbers R is a purely mathematical (imaginary) structure which we can use as a tool for many different purposes.

Plane coordinates. [pict9]. We fix two perpendicular intersecting lines, the point O of their intersection we call “the origin”. Each of these two lines must become a coordinate line (in the same way as it was described above). The scale e for each coordinate line is the same (but sometimes it’s more convenient to use different scales, we will not meet such examples in this book and in the next books). One coordinate line is called an Ox axis, and the other one is called an Oy axis (there is a freedom to choose which one is Ox , and which one is Oy). For each axis, the zero number 0 must be compared to the point O .



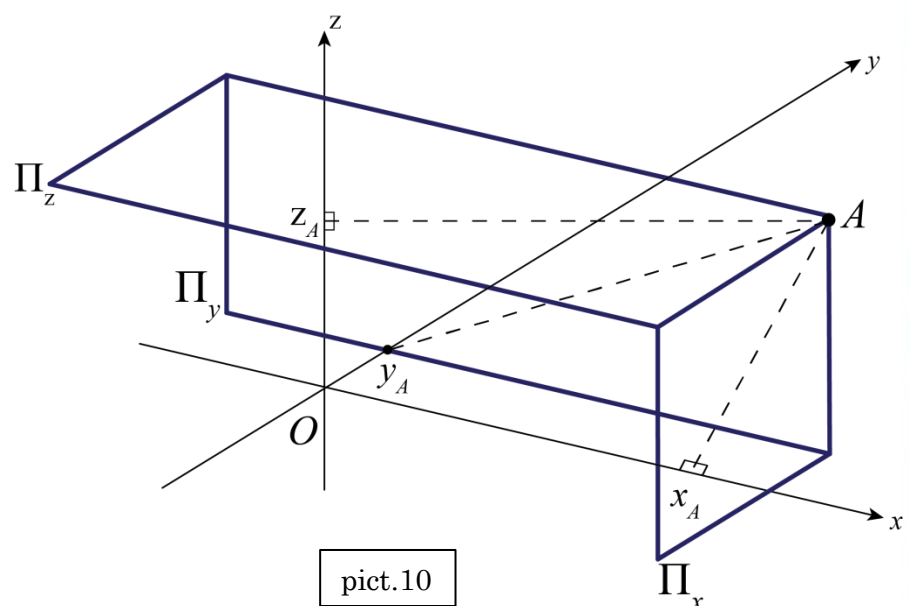
An important moment. We need to have a standard, according to which, we choose positive rays on the axes Ox and Oy . And this standard is our right hand’s palm. Look at the palm of Your right hand, when Your thumb is perpendicular to the forefinger. The hand must be put on the lines Ox, Oy : the thumb on Ox and the forefinger on Oy . The ray of Ox , which lies under the thumb, must be taken as a positive ray (of Ox), the ray of Oy , which lies under the forefinger, must be taken as a positive ray (of Oy). (notice, positive rays on Ox and Oy can be chosen in any other way, but it is not typical and no one really does it, at least intentionally).

Let’s mark any point A on the plane, we can draw the dashed lines, through this point which are perpendicular to Ox and Oy . By definition, coordinates of intersection points (x_A, y_A) (a pair of real numbers) are the coordinates of A . Conversely, any ordered pair (x_A, y_A) of real numbers uniquely defines exactly one point A on the plane (with coordinates (x_A, y_A))

When we write $A(5,3)$, we mean that A has coordinates $(5,3)$.

Space coordinates. [pict10]. We fix three perpendicular intersecting lines (in the space).

The point O of their intersection we call “the origin”. Each line must become a coordinate line, and for each line the zero number 0 must be compared to O . There is a freedom to choose which line is Ox , which is Oy and which is Oz . And again, we **need to use our standard**: we look at our right hand’s palm, the thumb is perpendicular to the forefinger, and the middle finger is perpendicular to the palm. Then, as earlier, we put the thumb on Ox , the forefinger on Oy and the middle finger on Oz .



Each finger lies on the ray which must be chosen as a positive ray of the axis.

Now we have the axes Ox, Oy, Oz . Let's mark any point A in the space. We draw the planes Π_x, Π_y, Π_z through the point A which are perpendicular to the axes Ox, Oy, Oz .

Then Π_x, Π_y, Π_z intersect Ox, Oy, Oz at some points with coordinates x_A, y_A, z_A , these coordinates must be taken as coordinates of A .

Conversely, any ordered set of real numbers (x_A, y_A, z_A) defines only one point A in the space (with coordinates (x_A, y_A, z_A)). In order to find the point A we need to mark the points with coordinates x_A, y_A, z_A on the axes Ox, Oy, Oz and to draw the planes Π_x, Π_y, Π_z through the marked points, which are perpendicular to Ox, Oy, Oz , these planes will intersect at the point A with coordinates (x_A, y_A, z_A) . When we write $A(1,3,5)$, we mean that A has coordinates $(1,3,5)$.

Square root and types of sets

Def. X is a set of real numbers. Any rule, that for every number $x \in X$ compares exactly one real number $f(x) \in R$, is called a function on X . Any number $x \in X$ can be called “a point x ” and $f(x)$ can be called “a value of f at a point x ”.

Def. $a \in X$ is any point (a number) of X . And f is a function which is defined on X .

If there exist some sequence $\{x_n\} \subset X \parallel x_n \neq a \ (\forall n), \{x_n\} \rightarrow a$, and for any such sequence the sequence $\{f(x_n)\}$ goes to $f(a)$, then we say “ f is continuous at a ”.

If there is no any sequence $\{x_n\} \subset X \parallel x_n \neq a \ (\forall n), \{x_n\} \rightarrow a$, then, by definition, we also say “ f is continuous at a ”.

Def: a function f is called continuous on X if f is defined on X and f is continuous at every point $a \in X$.

Assertion1. The power function $f(x) = x^k \parallel k \in \mathbb{N}$ is continuous on R .

Proof. Let's fix any point $a \in R$ and let's consider any sequence of real numbers $\{x_n\} \rightarrow a \parallel x_n \neq a \ (\forall n)$. According to the basic properties of convergent sequences, $(\{x_n\} \rightarrow a, \{y_n\} \rightarrow b \Rightarrow \{x_n \cdot y_n\} \rightarrow a \cdot b)$, we have $\{x_n\} \rightarrow a, \{x_n\} \rightarrow a \Rightarrow \{x_n^2\} \rightarrow a^2$, then $\{x_n^2\} \rightarrow a^2, \{x_n\} \rightarrow a \Rightarrow \{x_n^3\} \rightarrow a^3$ and etc.

Finally, $\{x_n^k\} \rightarrow a^k$, which is equivalent to $\{f(x_n)\}$ goes to $\{f(a)\}$, because $f(x) = x^k$, so f is continuous at every point $a \in R$, then f is continuous on R .

Theorem1 [A zero point of a continuous function]. f is continuous on $[a, b]$ and the values of f at the end points a, b have different signs: $f(a) < 0, f(b) > 0$ or $f(a) > 0, f(b) < 0$, then there exist some point $c \in (a, b)$ such that $f(c) = 0$.

Proof. Without loss of generality, let $f(a) < 0, f(b) > 0$. We divide the segment $[a, b]$ into two equal segments: $\left[a, \frac{a+b}{2}\right]$ and $\left[\frac{a+b}{2}, b\right]$. If f reaches zero at the middle point $\frac{a+b}{2}$, i.e.,

$f\left(\frac{a+b}{2}\right) = 0$, then the zero point c is found. If it's not the case, then one of the segments:

$\left[a, \frac{a+b}{2}\right]$ or $\left[\frac{a+b}{2}, b\right]$ has the same property as $[a, b]$, at the left end of that segment the value of f is negative, and at the right end of that segment the value of f is positive.

Let it be $\left[\frac{a+b}{2}, b\right] \equiv [a_1, b_1]$, then we divide it into two equal segments $\left[a_1, \frac{a_1+b_1}{2}\right]$ and $\left[\frac{a_1+b_1}{2}, b_1\right]$. If at the middle point $\frac{a_1+b_1}{2}$: $f\left(\frac{a_1+b_1}{2}\right) = 0$, then c is found, and if not, then one of the segments $\left[a_1, \frac{a_1+b_1}{2}\right]$ or $\left[\frac{a_1+b_1}{2}, b_1\right]$ has the same property as $[a_1, b_1]$, and we choose it as a new segment $[a_2, b_2]$. And again, we divide it into two equal segments and etc. If the process ended after several steps, then f reaches zero at the middle point of some segment $[a_k, b_k]$, and the point c is found. If the process didn't end after several steps, then we have the sequence of nested segments $[a, b] \supset [a_1, b_1] \supset [a_2, b_2] \supset \dots$. The length of each next segment is a half of a length of a previous one, therefore there exist the unique point c which belongs to every segment. Obviously $c \in [a, b]$, let's show that $f(c) = 0$. We assume that $f(c)$ is positive, then we can choose exactly one end point x_k of every segment $[a_k, b_k]$ (a_k or b_k) at which $f < 0$. The sequence $\{x_n\}$ of ends of segments goes to c , and f is continuous at c , then $\{f(x_n)\} \rightarrow f(c)$. But the negative sequence $\{f(x_n)\}$ can't go to the positive number $f(c)$, we have a contradiction. And similarly, if we assume that $f(c)$ is negative, then we can choose exactly one end point x_k of every segment $[a_k, b_k]$ at which $f > 0$, and we will get the similar contradiction. So $f(c) = 0$ and $c \in [a, b]$. According to the initial conditions, $c \neq a$ and $c \neq b$, then $c \in (a, b)$.

Consequence1 [intermediate values of a continuous function]. f is continuous on $[a, b]$.

Then f reaches all its intermediate values on this segment: for any number T between $f(a)$ and $f(b)$ there exist some point $c \in (a, b)$ such that $f(c) = T$.

Comment1. When we say that T is between $f(a)$ and $f(b)$, we mean that $f(a) < T < f(b)$ or $f(b) < T < f(a)$.

Comment2. f is continuous on $[a, b]$, then for any constant $T \in \mathbb{R}$ the function $T \pm f$ is continuous on $[a, b]$ (It immediately follows from the basic properties of sequences).

Proof. Without loss of generality, let $f(a) < f(b)$. Let's fix an arbitrary number $f(a) < T < f(b)$. Then we consider the auxiliary function $g(x) = T - f(x) \parallel x \in [a, b]$, this function (**comment2**) is continuous on $[a, b]$ and the values of $g(x)$ at the end points a, b have different signs: $g(a) = T - f(a) > 0$ and $g(b) = T - f(b) < 0$. Then, according to the **theorem1**, there exist some point $c \in (a, b)$ such that $g(c) = 0 \Leftrightarrow T - f(c) = 0 \Rightarrow f(c) = T$. The **consequence1** is proved.

Def. The real number $c \in \mathbb{R}$ is called a k -th root ($k \in \mathbb{N}$) of a if $c^k = a$. In such case we write $c = \sqrt[k]{a}$.

An integer number k is called even if k is divisible by 2, so k is even if $k = 2p$ for some $p \in \mathbb{N}$. An integer number k is called odd if k is not divisible by 2, so k is odd if $k = 2p + 1$ for some $p \in \mathbb{N}$.

Any integer number is even or odd and no other variants, it follows from the [theorem1,[part2],page66,(division with a remainder)] about divisibility of integer numbers.

Let's take the pair of integers $k, 2$, there exist the unique representation $k = 2 \cdot \bar{k} + r \parallel 0 \leq r < 2$, so the remainder r equals 0 or 1, if r is zero, then k is even, if r is one, then k is odd.

Theorem2.

[1] $a \in \mathbb{R}$ is a positive real number. For any even $k \in \mathbb{N}$ there exist exactly two different opposite values of $\sqrt[k]{a}$. For any odd $k \in \mathbb{N}$ there exist only one positive value of $\sqrt[k]{a}$.

[2] $a \in \mathbb{R}$ is a negative real number. For any even $k \in \mathbb{N}$ the value $\sqrt[k]{a}$ does not exist. For any odd $k \in \mathbb{N}$ there exist only one negative value of $\sqrt[k]{a}$.

Comment: it's easy to notice that this theorem doesn't have a "symmetrical form", so everything depends on the pair $a \in \mathbb{R}, k \in \mathbb{N}$, which is not a convenient thing. For complex numbers (which we will build in the next book) the situation is more symmetrical. For any non-zero complex number z there is always k different values of $\sqrt[k]{z}$ and for $z = 0$ only one value $\sqrt[k]{z} = 0$.

Proof. [1.1] Let's fix any positive $a \in \mathbb{R}$ and any even $k \in \mathbb{N}$.

Existence. Let's consider the function $f(x) \equiv x^k \parallel x \in \mathbb{R}$. If k is even, then $f(x) \equiv x^k \geq 0 \forall x \in \mathbb{R}$.

We consider any segment $[0, d] \parallel d > 1$ which contains a , so $0 < a < d$, then

$0 < a < d < d^k \Leftrightarrow 0 < a < d^k \Leftrightarrow f(0) < a < f(d)$. Then a is an intermediate value of $f(x) \equiv x^k$ on $[0, d]$, and $f(x)$ is continuous on $[0, d]$ (because $f(x) \equiv x^k$ is continuous on \mathbb{R}).

Then $f(x) \equiv x^k$ reaches the value a at some point $c \in (0, d)$ [consequence1], so $f(c) = a \Leftrightarrow c^k = a$, it means that c is a k -th root of a . And c is a positive number. For any even number k we have $(-c)^k = c^k$, then $(-c)^k = a$ and $-c$ is also a k -th root of a .

Uniqueness. Let's assume that there exist some other number d which is also a k -th root of a .

So $d \neq c$ and $d \neq -c$. From the condition $d^k = a$ follows that $(-d)^k = a$. One of the numbers $-d, d$ is positive, without loss of generality, let it be d . Let's compare d and c , if $d < c$, then $d^k < c^k = a$ and we have a contradiction, if $d > c$, then $d^k > c^k = a$ and we have a contradiction again. Then $d = c$, which contradicts to our initial assumption $d \neq c$. The uniqueness is proved.

[1.2] Let's fix any positive $a \in R$ and any **odd** $k \in \mathbb{N}$.

Existence. We consider again $f(x) \equiv x^k \parallel x \in R$ and any segment $[0, d] \parallel d > 1$ which

contains a . And again, (as we showed above), there exist $c \in (0, d)$ such that $c^k = a$, but now the number $-c$ is not appropriate, because $(-c)^k$ is negative (k is odd) and a is positive.

Uniqueness. Let there exist some other $d \neq c$ such that $d^k \neq a$. The number d can't be negative, because in this case $d^k < 0$, whereas a is positive, so d is positive.

And again, if $d < c \Rightarrow d^k < c^k = a$ and we have a contradiction, if $d > c \Rightarrow d^k > c^k = a$ and we have a contradiction again. So, there must be $d = c$ which contradicts to our initial assumption $d \neq c$. The uniqueness is proved.

[2.1] Let a is a negative real number, and $k \in \mathbb{N}$ is even. Let's assume that there exist $c \in R$ such that $c^k = a$. Obviously $c \neq 0$, then c is positive/negative. The number c^k is positive (because k is even) whereas a is negative, so there **can't be** $c^k = a$.

[2.2] Existence. Let a is a negative real number, and $k \in \mathbb{N}$ is odd. Let's consider the positive number $|a| > 0$. We have $a = -|a|$. According to **[1.1]**, for $|a| > 0$ there exist only one positive $c \in R$ such that $c^k = |a|$. Then $-c$ is a k -th root of a , really, $(-c)^k = [k \text{ is odd}] = -c^k = -|a| = a$.

Uniqueness. Let's assume that there exist some other k -th root of a . So $d^k = a = -|a|$.

Then $(-d)^k = |a|$ where $|a|$ is positive, then $-d = c$ (from **[2.2]**), then $d = -c$ (from **[2.2]**).

The uniqueness is proved.

And finally, for $a = 0$ and for any natural $k \in \mathbb{N}$ we obviously have $\sqrt[k]{a} = 0$.

Let's make a **very important agreement**. For any positive $a \in R$ and any **even** $k \in \mathbb{N}$, we agree that the symbol $\sqrt[k]{a}$ denotes the positive value of k -th root. If we want to denote the negative value of k -th root, we will write $-\sqrt[k]{a}$.

Let's consider any points $A(x_A, y_A)$ and $B(x_B, y_B)$ on the plane. The segment AB (in general) is a diagonal of a rectangle, which sides have lengths $|x_B - x_A|$ and $|y_B - y_A|$.

From the Pythagorean theorem follows that $AB = \sqrt{|x_B - x_A|^2 + |y_B - y_A|^2}$. Similarly, for any points

$A(x_A, y_A, z_A)$ and $B(x_B, y_B, z_B)$ in the space, the segment AB (in general) is a diagonal of

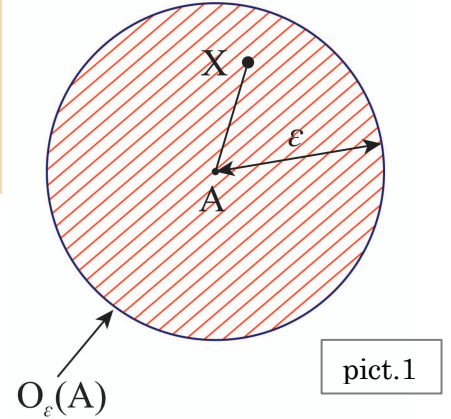
a rectangular parallelepiped, which sides have lengths $|x_B - x_A|$ and $|y_B - y_A|$ and $|z_B - z_A|$.

By using the Pythagorean theorem two times we get: $AB = \sqrt{|x_B - x_A|^2 + |y_B - y_A|^2 + |z_B - z_A|^2}$.

For convenience we do not say “the segment AB has a length a ”, but only

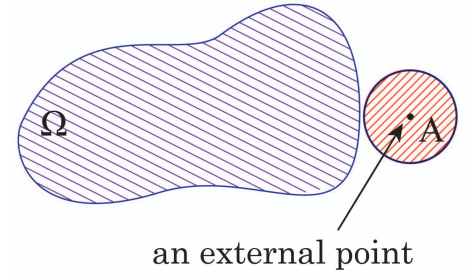
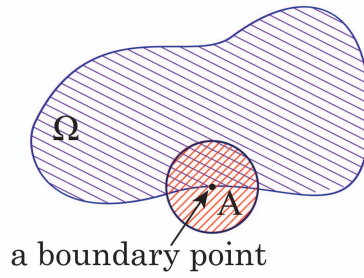
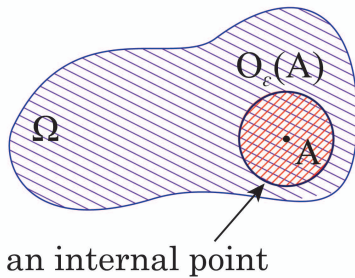
“the segment AB is a ”. We can say for example, “the rectangle Π with sides a, b ”.

Def. Let A is any point on the plane and $\varepsilon > 0$ is a fixed positive number. The ε -neighborhood $O_\varepsilon(A)$, or just a neighborhood of A , is the set $O_\varepsilon(A) \equiv \{X \mid AX < \varepsilon\}$. [pict1].



And for any point A in the space, there is a similar definition. And from now on, any set of points Ω on the plane/in the space we will call “a figure Ω ”.

Def: a point A is called an internal point of Ω if A belongs to Ω together with some neighborhood $O_\varepsilon(A)$. So A is an internal point of $\Omega \Leftrightarrow$ There exist $O_\varepsilon(A)$ such that $O_\varepsilon(A) \subset \Omega$ [pict2]. A is called a boundary point of Ω if **any** neighborhood $O_\varepsilon(A)$ contains one point from Ω and one point not from Ω [pict3]. And finally, A is called an external point of Ω if A doesn't belong to Ω together with some neighborhood $O_\varepsilon(A)$ [pict4].



Exercise. Let Ω is any fixed figure on the plane/in the space. Then for any point A exactly one of the next cases is true: **[A]** A is an internal point of Ω . **[B]** A is a boundary point of Ω . **[C]** A is an external point of Ω .

Notice: any internal point of Ω always belongs to Ω , any boundary point of Ω may belong and may not belong to Ω , any external point of Ω doesn't belong to Ω .

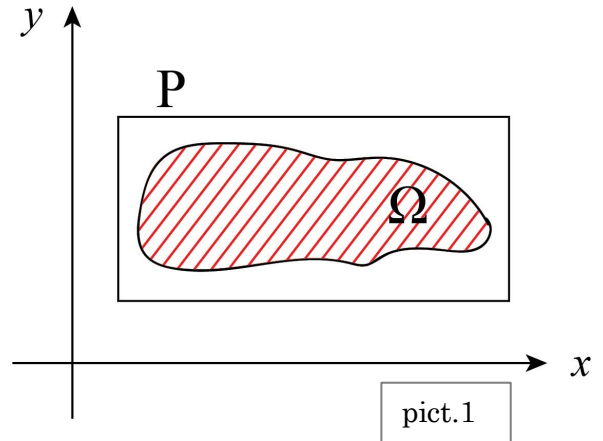
Def: a set of all internal points of Ω is called an interior of Ω , and we denote it $\text{int } \Omega$, a set of all boundary points of Ω is called a boarder of Ω , and we denote it $\partial\Omega$.

Area construction

Let's fix some plane Π and any coordinate system Oxy on this plane. From now on, we work only on the plane Π .

Def1. A figure Ω is called bounded if there exist some rectangle $P \supset \Omega$ which sides are parallel to coordinate axes Ox, Oy [pict1]. From now on we work only with bounded figures on the plane.

Def2. Figures Ω, Ψ are called equal if there exist one-to-one mapping $f: \Omega \rightarrow \Psi$ which conserves distances and parallelism: $\forall A, B \in \Omega$ the segment AB is equal to the segment $f(A)f(B)$ and the line AB is parallel to the line $f(A)f(B)$.



Def3. The area S is the correspondence $S: X \rightarrow R^+ \cup \{0\}$ that is defined on the collection X of plane-figures, these plane figures are called measurable. For every concrete figure $\Omega \subset X$ a unique non-negative number $S(\Omega)$ is defined, $S(\Omega)$ is called an area of Ω .

And $S: X \rightarrow R^+ \cup \{0\}$ has the next properties:

[1] The area of **any** unit square, which sides are parallel to coordinate axes, is 1, so $S(1 \times 1) = 1$

[2] If measurable figures Ω, Ψ do not have any common internal points, then $S(\Omega \cup \Psi) = S(\Omega) + S(\Psi)$.

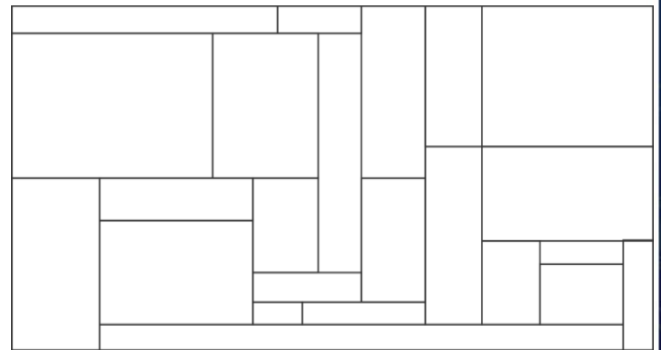
[3] If measurable figures Ω, Ψ are equal, then $S(\Omega) = S(\Psi)$.

Comment. The question about the existence of such correspondence is very important.

In most of books the area or (measure) is defined in the next way: by definition the area of any rectangle (or parallelepiped) is defined as a product of it's sides, and after that the next theory appears. Such approach has a huge flaw. If we assume that the area of any rectangle (which sides are parallel to coordinate axes) is a product of it's sides, we automatically define the area on the huge class of figures, i.e., on the class of rectangles. How can we check now that the property **[2]** (additivity of area) is still in power?

Really, there are a lot of intricate ways to divide any rectangle into several rectangles without common internal points [pict2], and it's not obvious at all why

the area of a big rectangle is a sum of areas of smaller rectangles. And such approach implies that

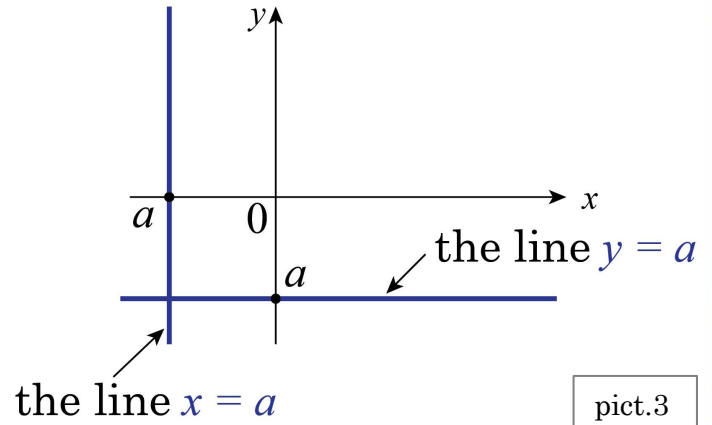


we just have to believe that the additivity [2] is still true. There will be given a normal construction of area which doesn't have this flaw.

Construction process.

Let's fix any coordinate system Oxy .

For any $a \in \mathbb{R}$, the line $x = a$ is the set of points with coordinates $\{(x, y) \mid x = a, y \in \mathbb{R}\}$ [pict3], and the line $y = a$ is the set of points with coordinates $\{(x, y) \mid x \in \mathbb{R}, y = a\}$.



pict.3

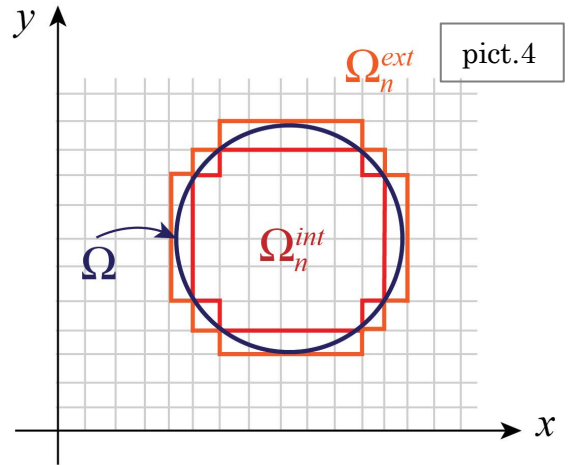
For any natural number $n \in \mathbb{N}$ we consider the “quadratic net”, i.e., the set of all lines on the plane with equations $x = k \cdot 10^{-n}$, $y = k \cdot 10^{-n} \mid k \in \mathbb{Z}$.

Such net divides the plane into equal squares, and the greater the number n , the “thicker” the net.

Let Ω is any **bounded** figure. Let's fix any number $n \in \mathbb{N}$ and the net $x = k \cdot 10^{-n}$, $y = k \cdot 10^{-n} \mid k \in \mathbb{Z}$.

Let Ω_n^{int} is the figure that consists of all squares which completely belong to Ω , so Ω_n^{int} consists of T_n squares (T_n is some non-negative integer number).

Next, Ω_n^{ext} is the figure that consists of all squares which have at least one common point with Ω , so Ω_n^{ext} consists of H_n squares (H_n is some non-negative integer number).



pict.4

For any natural n we obviously have $\Omega_n^{\text{int}} \subset \Omega \subset \Omega_n^{\text{ext}}$ [pict4] and $T_n \leq H_n$.

We will say that Ω_n^{int} is an internal quadratic figure (for Ω) and Ω_n^{ext} is an external quadratic figure (for Ω). For any n we define the internal sum $\Sigma_n^{\text{int}} = T_n \cdot 10^{-2n}$ and the external sum $\Sigma_n^{\text{ext}} = H_n \cdot 10^{-2n}$. So, for any n we have $\Sigma_n^{\text{int}} \leq \Sigma_n^{\text{ext}}$. It's very important to notice here: as Ω is bounded (def1), then for any $n \in \mathbb{N}$ the internal and external sums are concrete real (even rational) numbers. And therefore, we have two sequences $\{\Sigma_n^{\text{int}}\}$ and $\{\Sigma_n^{\text{ext}}\}$.

Assertion1. Ω is any figure on the plane. Then the sequence of internal sums $\{\Sigma_n^{\text{int}}\}$ is monotonically increasing ($\Sigma_n^{\text{int}} \leq \Sigma_{n+1}^{\text{int}} \mid \forall n$) and the sequence of external sums $\{\Sigma_n^{\text{ext}}\}$ is monotonically decreasing ($\Sigma_{n+1}^{\text{ext}} \leq \Sigma_n^{\text{ext}} \mid \forall n$).

Any internal sum is not greater than any external sum: $\Sigma_n^{\text{int}} \leq \Sigma_m^{\text{ext}} \mid \forall m, n \in \mathbb{N}$.

Proof. Let's fix any bounded figure Ω and let's build a quadratic net for some $n \in \mathbb{N}$. This net defines the internal figure Ω_n^{int} and the internal sum $\Sigma_n^{\text{int}} = T_n \cdot 10^{-2n}$, where T_n is the number of net-squares in Ω_n^{int} . Let's consider the net for the number $n+1$. Every square of Ω_n^{int} is divided into 100 smaller squares, these squares are still completely belong to Ω , therefore $\Omega_n^{\text{int}} \subset \Omega_{n+1}^{\text{int}}$. Each square, which is counted in T_n , gives 100 squares for T_{n+1} , then $100 \cdot T_n \leq T_{n+1}$. Then $\Sigma_{n+1}^{\text{int}} = T_{n+1} \cdot 10^{-2(n+1)} \geq (100 \cdot T_n) \cdot 10^{-2(n+1)} = T_n \cdot 10^{-2n} = \Sigma_n^{\text{int}}$, so $\Sigma_{n+1}^{\text{int}} \geq \Sigma_n^{\text{int}} \parallel \forall n$. And similarly we can show $\Sigma_{n+1}^{\text{ext}} \leq \Sigma_n^{\text{ext}} \parallel \forall n$.

So, the sequence $\{\Sigma_n^{\text{int}}\}$ is monotonically increasing and $\{\Sigma_n^{\text{ext}}\}$ is monotonically decreasing.

Next, let $m = n$, then the inequality $\Sigma_n^{\text{int}} \leq \Sigma_m^{\text{ext}}$ is obvious. Let $m > n$, then $\Sigma_n^{\text{int}} \leq \Sigma_m^{\text{int}} \leq \Sigma_m^{\text{ext}}$.

Let finally $n > m$, then $\Sigma_n^{\text{int}} \leq \Sigma_n^{\text{ext}} \leq \Sigma_m^{\text{ext}}$.

From $\Sigma_n^{\text{int}} \leq \Sigma_m^{\text{ext}} \parallel \forall m, n \in \mathbb{N}$ immediately follows that the sequence $\{\Sigma_n^{\text{int}}\}$ is bounded above (by any concrete term of the sequence of external sums) and $\{\Sigma_n^{\text{ext}}\}$ is bounded below (by any concrete term of the sequence of internal sums), then (the theorem about a limit of a monotonic sequence) both these sequences converge $\{\Sigma_n^{\text{int}}\} \rightarrow S_{\text{low}}$ and $\{\Sigma_n^{\text{ext}}\} \rightarrow S_{\text{up}}$.

Def4. If $S_{\text{low}} = S_{\text{up}}$, then Ω is called **measurable** and the number $S(\Omega) \equiv S_{\text{low}} = S_{\text{up}}$ is called an area of Ω .

The main theorem.

The area of any rectangle, which sides a, b are parallel to coordinate axes, equals $a \cdot b$.

The proof of this theorem can't be done quickly, the reason is that everything depends on the "position" of such rectangle. If it's vertexes have "good" coordinates, the proof is quite simple. But if we want to prove this theorem for any rectangle, we need to derive at first some auxiliary properties and assertions.

Assertion2 [additivity of area]. Let Ω, Ψ are measurable figures without common internal points, then $S(\Omega \cup \Psi) = S(\Omega) + S(\Psi)$.

Proof. Let's fix any $n \in \mathbb{N}$ and build a quadratic net for $n \in \mathbb{N}$. This net defines the internal and external quadratic figures $\Omega_n^{\text{int}} \subset \Omega_n^{\text{ext}}, \Psi_n^{\text{int}} \subset \Psi_n^{\text{ext}}$. Let's also consider the internal and external quadratic figures for $\Omega \cup \Psi$, so $(\Omega \cup \Psi)_n^{\text{int}} \subset (\Omega \cup \Psi)_n^{\text{ext}}$. Any square from $(\Omega \cup \Psi)_n^{\text{ext}}$ is a square that has a common point with Ω or with Ψ (or with Ω and with Ψ). Such square for sure belongs to the union $\Omega_n^{\text{ext}} \cup \Psi_n^{\text{ext}}$, then we have $(\Omega \cup \Psi)_n^{\text{ext}} \subset \Omega_n^{\text{ext}} \cup \Psi_n^{\text{ext}}$. Then the number of squares in $(\Omega \cup \Psi)_n^{\text{ext}}$ is not greater than the number of squares in $\Omega_n^{\text{ext}} \cup \Psi_n^{\text{ext}}$, and the number of squares in $\Omega_n^{\text{ext}} \cup \Psi_n^{\text{ext}}$ obviously is not greater than the number of squares in Ω_n^{ext} plus the number of squares

in Ψ_n^{ext} . Then: $[the\ number\ of\ squares\ in\ (\Omega \cup \Psi)_n^{ext}] \leq [the\ number\ of\ squares\ in\ \Omega_n^{ext}] + [the\ number\ of\ squares\ in\ \Psi_n^{ext}] \Leftrightarrow H_n(for\ \Omega \cup \Psi) \leq H_n(for\ \Omega) + H_n(for\ \Psi)$ [T1].

Let's consider now Ω_n^{int} and Ψ_n^{int} . Any square from Ω_n^{int} is a square that belongs to Ω and therefore it belongs to $\Omega \cup \Psi$, then it belongs to $(\Omega \cup \Psi)_n^{int}$, then all Ω_n^{int} belongs to $(\Omega \cup \Psi)_n^{int}$. And similarly, Ψ_n^{int} belongs to $(\Omega \cup \Psi)_n^{int}$. Then the union $\Omega_n^{int} \cup \Psi_n^{int}$ belongs to $(\Omega \cup \Psi)_n^{int}$. Then the number of squares in $\Omega_n^{int} \cup \Psi_n^{int}$ is not greater than the number of squares in $(\Omega \cup \Psi)_n^{int}$. Let's notice that figures $\Omega_n^{int}, \Psi_n^{int}$ do not have any common squares, because if they have a common square, then it's center is a common internal point of Ω, Ψ , and these figures do not have any common internal points. Then:

$[the\ number\ of\ squares\ in\ \Omega_n^{int} \cup \Psi_n^{int}] = [the\ number\ of\ squares\ in\ \Omega_n^{int}] + [the\ number\ of\ squares\ in\ \Psi_n^{int}]$ and, as we noticed above, the number of squares in $\Omega_n^{int} \cup \Psi_n^{int}$ is not greater than the number of squares in $(\Omega \cup \Psi)_n^{int}$, then:

$$[the\ number\ of\ squares\ in\ \Omega_n^{int}] + [the\ number\ of\ squares\ in\ \Psi_n^{int}] \leq [the\ number\ of\ squares\ in\ (\Omega \cup \Psi)_n^{int}] \Leftrightarrow T_n(for\ \Omega) + T_n(for\ \Psi) \leq T_n(for\ \Omega \cup \Psi)$$
 [T2].

And finally, for $\Omega \cup \Psi$ (as for any other figure), the number of squares that belong to $\Omega \cup \Psi$ is not greater than the number of squares that have a common point with $\Omega \cup \Psi$, i.e.,

$T_n(for\ \Omega \cup \Psi) \leq H_n(for\ \Omega \cup \Psi)$ [T3]. From [T1],[T2],[T3] we have:

$T_n(for\ \Omega) + T_n(for\ \Psi) \leq T_n(for\ \Omega \cup \Psi) \leq H_n(for\ \Omega \cup \Psi) \leq H_n(for\ \Omega) + H_n(for\ \Psi)$ let's multiply all the sides by 10^{-2n} , we will get:

$\Sigma_n^{int}(for\ \Omega) + \Sigma_n^{int}(for\ \Psi) \leq \Sigma_n^{int}(for\ \Omega \cup \Psi) \leq \Sigma_n^{ext}(for\ \Omega \cup \Psi) \leq \Sigma_n^{ext}(for\ \Omega) + \Sigma_n^{ext}(for\ \Psi)$ [T4].

We know that figures Ω, Ψ are measurable, by definition it means that

$\lim_{n \rightarrow \infty} \{\Sigma_n^{int}(for\ \Omega)\} = \lim_{n \rightarrow \infty} \{\Sigma_n^{ext}(for\ \Omega)\} \equiv //\ by\ def\ // \equiv S(\Omega)$ and

$\lim_{n \rightarrow \infty} \{\Sigma_n^{int}(for\ \Psi)\} = \lim_{n \rightarrow \infty} \{\Sigma_n^{ext}(for\ \Psi)\} \equiv //\ by\ def\ // \equiv S(\Psi)$.

Then in [T4] the outer sequences have equal limits:

$\Sigma_n^{int}(for\ \Omega) + \Sigma_n^{int}(for\ \Psi) \xrightarrow{n \rightarrow \infty} S(\Omega) + S(\Psi)$ and

$\Sigma_n^{ext}(for\ \Omega) + \Sigma_n^{ext}(for\ \Psi) \xrightarrow{n \rightarrow \infty} S(\Omega) + S(\Psi)$. Let's apply the squeeze theorem for sequences:

both sequences $\{\Sigma_n^{int}(for\ \Omega \cup \Psi)\}$ and $\{\Sigma_n^{ext}(for\ \Omega \cup \Psi)\}$ converge to $S(\Omega) + S(\Psi)$, then (by definition) $\Omega \cup \Psi$ is measurable and it's area is $S(\Omega) + S(\Psi)$.

Assertion3. There is a rectangle Π on the plane with sides a, b , and each vertex of Π has coordinates $\left(\frac{m}{10^{\tilde{k}}}, \frac{n}{10^{\bar{k}}}\right)$, where $m, n \in \mathbb{Z}$, $\tilde{k}, \bar{k} \in \mathbb{N}$, then the area of such rectangle equals $a \cdot b$.

Proof. Each coordinate of each vertex has a denominator $10^{\bar{k}} \parallel \bar{k} \in \mathbb{N}$. Let's choose the maximal power $k_{\max} \equiv k$ among all 8 denominators. Then each coordinate of each vertex can be written as a fraction with the denominator 10^k . Let's build the quadratic net for that number k .

As each coordinate of each vertex of Π is a fraction $\frac{h}{10^k} \parallel h \in \mathbb{Z}$, then each side of Π must lie on some line of the quadratic net for k . Let's notice that if we build the quadratic net for the next number $k+1$ all the lines of the net for k are still present in the net for $k+1$, but in addition we will have multiple new lines. Then the sides of Π lie on the lines of any quadratic net which is built for $n \geq k$.

Let's fix an arbitrary natural number $n \geq k$ and build the quadratic net for n . We choose the vertex of Π which x and y coordinates are both minimal. Let's denote it $\left(\frac{m_{\min}}{10^n}, \frac{n_{\min}}{10^n}\right)$, then the other vertexes must have coordinates

$$\left(\frac{m_{\min}}{10^n} + b, \frac{n_{\min}}{10^n}\right), \left(\frac{m_{\min}}{10^n}, \frac{n_{\min}}{10^n} + a\right), \left(\frac{m_{\min}}{10^n} + b, \frac{n_{\min}}{10^n} + a\right).$$

Let's find internal and external quadratic figures and internal and external sums for Π .

[Internal sum]

The internal quadratic figure Ω_n^{int} [pict5] comprises all the squares which belong to Π .

Let's find the number of squares T_n in the internal figure.

The number of net-squares in any row, which is parallel to Ox , is $\frac{b}{10^n}$.

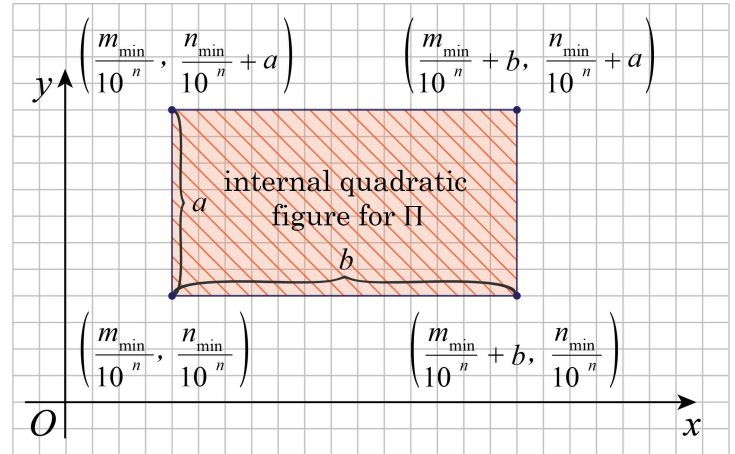
The number of net-squares in any row, which is parallel to Oy , is $\frac{a}{10^n}$.

Then the number of net-squares in Π is

$$\frac{a}{10^n} \cdot \frac{b}{10^n} = \frac{a \cdot b}{10^{2n}}.$$

Therefore, the internal sum for Π is

$$\Sigma_n^{\text{int}} = (\text{the total number of squares}) \cdot 10^{-2n} = \frac{a \cdot b}{10^{2n}} \cdot 10^{-2n} = a \cdot b \text{ [V]}$$



pict.5

[External sum]

The external quadratic figure Ω_n^{ext} [pict6] comprises all the squares which belong to Π plus all the squares which “stay around” Π . There are two lateral strips of squares, which are “parallel” to Ox (blue colour), each strip consists of $\frac{b}{10^n}$ squares, so these strips give $2 \cdot \frac{b}{10^n}$ squares.

There are two lateral strips of squares which are “parallel” to Oy (green colour), each strip consists of $\frac{a}{10^n}$ squares, and these strips give $2 \cdot \frac{a}{10^n}$ squares.

And we also have exactly 4 squares (gray colour), each of these square has a common vertex with Π . So there are exactly $2 \cdot \frac{b}{10^n} + 2 \cdot \frac{a}{10^n} + 4$ squares “around” Π .

The external sum Σ_n^{ext} here differs from the internal Σ_n^{int} sum only by summands which appear because of the surrounding squares. All the summands from the internal sum present in the external sum. Then, according to [V]:

$$\Sigma_n^{ext} = a \cdot b + \left(2 \cdot \frac{b}{10^n} + 2 \cdot \frac{a}{10^n} + 4 \right) \cdot 10^{-2n} = a \cdot b + (2b \cdot 10^{-n} + 2a \cdot 10^{-n} + 4 \cdot 10^{-n}) \text{ [V1]}.$$

The formulas [V] and [V1] are true for any $n \geq k$, and we are interested in the next two limits:

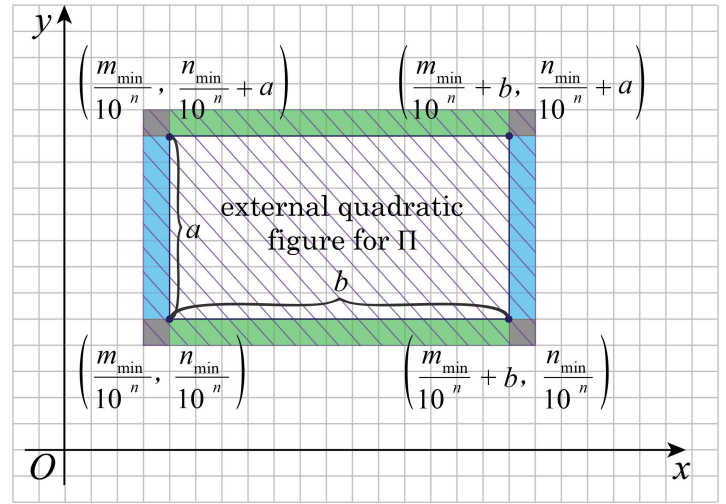
$$\begin{aligned} \lim_{n \rightarrow \infty} \Sigma_n^{int} &= //[\text{V}]// = \lim_{n \rightarrow \infty} a \cdot b = a \cdot b \text{ (because } a \cdot b = \text{const) and} \\ \lim_{n \rightarrow \infty} \Sigma_n^{ext} &= //[\text{V1}]// = \lim_{n \rightarrow \infty} (a \cdot b + (2b \cdot 10^{-n} + 2a \cdot 10^{-n} + 4 \cdot 10^{-n})) = \lim_{n \rightarrow \infty} a \cdot b + \\ &\lim_{n \rightarrow \infty} (2b \cdot 10^{-n} + 2a \cdot 10^{-n} + 4 \cdot 10^{-n}) = \lim_{n \rightarrow \infty} a \cdot b + 0 = a \cdot b. \end{aligned}$$

Then the sequence of external and internal sums for Π both go to the same limit $a \cdot b$, therefore (by definition) Π is measurable and $S(\Pi) = a \cdot b$.

Consequence 1. From the [assertions 2,3](#) follows that the area of any internal/external quadratic figure $\Omega_n^{int}, \Omega_n^{ext}$ is equal to the sum of areas of the net squares that form $\Omega_n^{int}, \Omega_n^{ext}$.

And therefore, any internal/external $\Sigma_n^{int}, \Sigma_n^{ext}$ sum is exactly the area of an internal/external quadratic figure: $\Sigma_n^{int} = S(\Omega_n^{int})$, $\Sigma_n^{ext} = S(\Omega_n^{ext})$.

Let's explain. Let's fix any quadratic net $n \in \mathbb{N}$, any net-square has coordinates of vertexes like in the [assertion 3](#). The sides of such square are both equal to 10^{-n} , then it's area is $10^{-n} \cdot 10^{-n} = 10^{-2n}$. Let's fix any figure Ω , then the figures $\Omega_n^{int}, \Omega_n^{ext}$ are defined, both these figures consist of some net-squares that do not have any common internal points, then, by additivity ([assertion 2](#)), the area of each figure $\Omega_n^{int}, \Omega_n^{ext}$ is a sum of areas of all squares which form this figure.



pict.6

There are T_n squares in Ω_n^{int} with area 10^{-2n} each, then the area of Ω_n^{int} is $T_n \cdot 10^{-2n}$ - but this number is exactly the internal sum Σ_n^{int} .

And similarly, the area of Ω_n^{ext} is exactly the external sum Σ_n^{ext} .

Then the definition of a measurable figure can be formulated now in the next way:

Def5: a figure Ω is called measurable if the sequence of areas of internal quadratic figures $\{S(\Omega_n^{\text{int}})\}$ and the sequence of areas of external quadratic figures $\{S(\Omega_n^{\text{ext}})\}$ both go to the same limit, that limit must be taken as $S(\Omega)$.

There is even a stronger assertion ([assertion5](#)) which has a great practical value.

Assertion4 [1-st criterion of measurability].

Ω is measurable \Leftrightarrow For any positive $\varepsilon > 0$ there exist **some** measurable figures M^{int} and M^{ext} such that $M^{\text{int}} \subset \Omega \subset M^{\text{ext}}$ and $S(M^{\text{ext}}) - S(M^{\text{int}}) < \varepsilon$.

Proof. \Rightarrow Let Ω is measurable, then [Def5] both sequences $\{S(\Omega_n^{\text{ext}})\}$ and $\{S(\Omega_n^{\text{int}})\}$ go to the same limit $S(\Omega)$. Let's fix any $\varepsilon > 0$, according to the simplest properties of limits, $\varepsilon/2$ neighborhood of $S(\Omega)$ contains all the terms of both sequences $\{S(\Omega_n^{\text{ext}})\}$ and $\{S(\Omega_n^{\text{int}})\}$, starting from some number k . Let's fix any $m > k \Rightarrow S(\Omega_m^{\text{int}}) \in O_{\varepsilon/2}(S(\Omega))$ and $S(\Omega_m^{\text{ext}}) \in O_{\varepsilon/2}(S(\Omega))$.

The difference of any two numbers, which are taken from any $\varepsilon/2$ neighborhood, is not greater than ε . Then $S(\Omega_m^{\text{ext}}) - S(\Omega_m^{\text{int}}) < \varepsilon$. Then $\Omega_m^{\text{ext}}, \Omega_m^{\text{int}}$ are the figures we need.

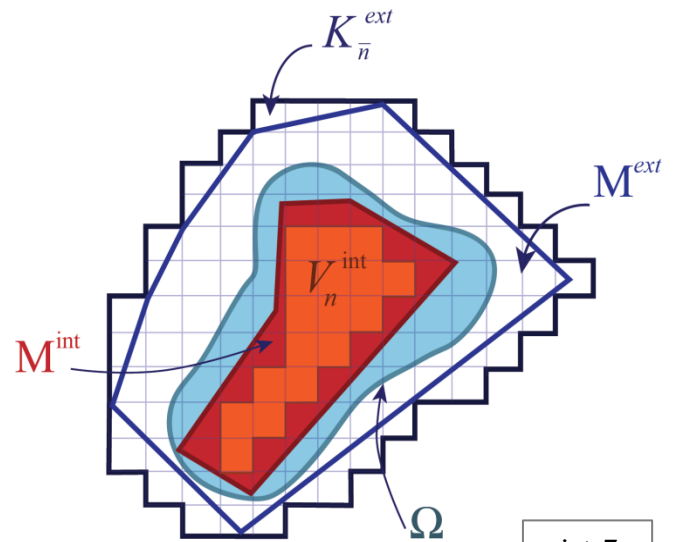
Conversely. \Leftarrow Let's fix an arbitrary $\varepsilon > 0$.

For the positive number $\varepsilon/4$ there exist some measurable figures M^{int} and M^{ext} such that $M^{\text{int}} \subset \Omega \subset M^{\text{ext}}$ and $S(M^{\text{ext}}) - S(M^{\text{int}}) < \varepsilon/4$ [E0].

As M^{ext} is measurable, there exist $\bar{n} \in \mathbb{N}$ and the external quadratic figure $K_{\bar{n}}^{\text{ext}} \supset M^{\text{ext}}$ such that $S(K_{\bar{n}}^{\text{ext}}) - S(M^{\text{ext}}) < \varepsilon/4$ [pict7].

As M^{int} is measurable, there exist $\tilde{n} \in \mathbb{N}$ and the internal quadratic figure $V_{\tilde{n}}^{\text{int}} \subset M^{\text{int}}$ such that $S(M^{\text{int}}) - S(V_{\tilde{n}}^{\text{int}}) < \varepsilon/4$. We got two important inequalities for not necessary equal \bar{n}, \tilde{n} , we fix any

number $m > \bar{n}, m > \tilde{n}$. Let's notice that when we take the greater number which defines the net, the area of any internal quadratic figure may only become greater and the area of any external quadratic figure may only become less.



pict.7

Then for the number m we have $K_m^{ext} \supset M^{ext}$ and $S(K_m^{ext}) - S(M^{ext}) < \varepsilon/4$ [E1]

(because $S(K_{\bar{n}}^{ext}) \geq S(K_m^{ext}) \geq S(M^{ext})$) and also $S(M^{int}) - S(V_m^{int}) < \varepsilon/4$ [E2]

(because $S(V_{\bar{n}}^{int}) \leq S(V_m^{int}) \leq S(M^{int})$).

Let's sum the inequalities [E0],[E1],[E2], then we get $S(K_m^{ext}) - S(V_m^{int}) < 3\varepsilon/4$ [E3].

Let's notice that the external quadratic figure Ω_m^{ext} (for Ω) must belong to K_m^{ext} and therefore $S(\Omega_m^{ext}) \leq S(K_m^{ext})$ and the internal quadratic figure V_m^{int} must belong to Ω_m^{int} (for Ω), then $S(V_m^{int}) \leq S(\Omega_m^{int})$. Let's sum up: $S(V_m^{int}) \leq S(\Omega_m^{int}) \leq S(\Omega_m^{ext}) \leq S(K_m^{ext})$.

And we also have [E3], from [E3] immediately follows $S(\Omega_m^{ext}) - S(\Omega_m^{int}) < 3\varepsilon/4 < \varepsilon$.

We showed that for any (small) positive $\varepsilon > 0$ we can find some natural m , such that

$S(\Omega_m^{ext}) - S(\Omega_m^{int}) < \varepsilon$ [U]. Let's notice now that the sequence of areas of internal figures $\{S(\Omega_n^{int})\}$

is monotonically increasing (because this sequence is exactly the sequence of internal sums $\{\Sigma_n^{int}\}$ and this sequence is monotonically increasing ([assertion1](#))). And the sequence of areas of external figures $\{S(\Omega_n^{ext})\}$ is monotonically decreasing. Both these sequences converge in any case, just

because Ω is a bounded figure: $\{S(\Omega_n^{int})\} \rightarrow S_{low}$ and $\{S(\Omega_n^{ext})\} \rightarrow S_{up}$. We obviously have:

$S(\Omega_n^{int}) \leq S_{low} \parallel \forall n$ and $S_{up} \leq S(\Omega_n^{ext}) \parallel \forall n$ and $S_{low} \leq S_{up}$ (because every term of the sequence $\{S(\Omega_n^{int})\}$ is not greater than every term of the sequence $S(\Omega_n^{ext})$). Then for any n we have

$S(\Omega_n^{ext}) - S(\Omega_n^{int}) \geq S_{up} - S_{low} \geq 0$, the difference $S_{up} - S_{low}$ is a constant and from [U] we see that this constant can be less than any positive number ε , then $S_{up} - S_{low} = 0$ and $S_{up} = S_{low}$.

Then, by definition, the figure Ω is measurable and the number $S(\Omega) \equiv S_{up} = S_{low}$ is defined.

Auxiliary1. Both figures Ψ, Ω are measurable and $\Psi \subset \Omega$, then $S(\Psi) \leq S(\Omega)$.

Proof. From $\Psi \subset \Omega$ immediately follows that $\Psi_n^{int} \subset \Omega_n^{int} \forall n \in \mathbb{N}$ then for any $n \in \mathbb{N}$ the number of net-squares in Ψ_n^{int} is not greater than the number of net squares in Ω_n^{int} .

As areas of Ψ_n^{int} and Ω_n^{int} are sums of areas of net-squares which form these figures (consequence1),

then $S(\Psi_n^{int}) \leq S(\Omega_n^{int})$ [J]. As figures Ψ, Ω are measurable, then $\{S(\Psi_n^{int})\} \rightarrow S(\Psi)$ and

$S(\Omega_n^{int}) \rightarrow S(\Omega)$ from [J] and from the basic properties of limits follows that $S(\Psi) \leq S(\Omega)$.

Asserrtion5 [2-nd criterion of measurability].

If there exist some sequence of measurable internal figures $\{M_n^{\text{int}}\} \parallel M_n^{\text{int}} \subset \Omega \forall n$ and some sequence of measurable external figures $\{M_n^{\text{ext}}\} \parallel \Omega \subset M_n^{\text{ext}} \forall n$ such that

$\lim_{n \rightarrow \infty} S(M_n^{\text{int}}) = \lim_{n \rightarrow \infty} S(M_n^{\text{ext}})$ [pict8], then Ω is

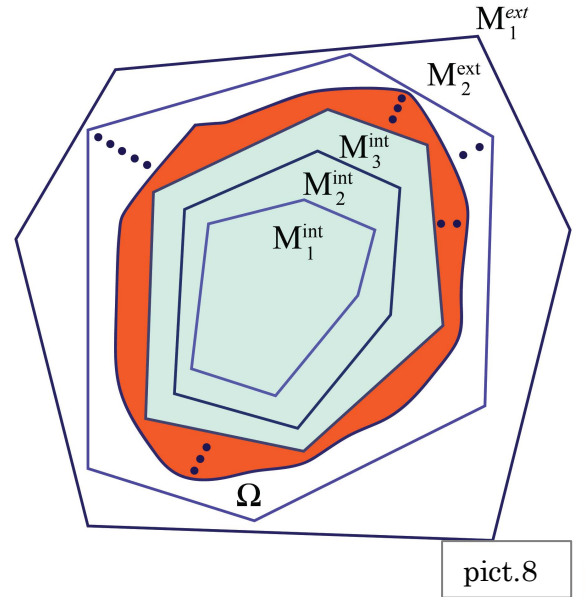
measurable and $S(\Omega) = \lim_{n \rightarrow \infty} S(M_n^{\text{int}}) = \lim_{n \rightarrow \infty} S(M_n^{\text{ext}})$

And conversely. If Ω is measurable, then there exist some sequence of measurable internal figures

$\{M_n^{\text{int}}\} \parallel M_n^{\text{int}} \subset \Omega \forall n$ and some sequence of measurable

external figures $\{M_n^{\text{ext}}\} \parallel \Omega \subset M_n^{\text{ext}} \forall n$ such that

$S(\Omega) = \lim_{n \rightarrow \infty} S(M_n^{\text{int}}) = \lim_{n \rightarrow \infty} S(M_n^{\text{ext}})$.



Proof. \Leftarrow The converse assertion is obvious, it immediately follows from the (def5), the sequences of internal and external quadratic figures are the sequences we need:

$\{\Omega_n^{\text{int}}\} \equiv \{M_n^{\text{int}}\}$ and $\{\Omega_n^{\text{ext}}\} \equiv \{M_n^{\text{ext}}\}$. Let's prove the other one \Rightarrow .

We denote $\Delta \equiv \lim_{n \rightarrow \infty} S(M_n^{\text{int}}) = \lim_{n \rightarrow \infty} S(M_n^{\text{ext}})$. Let's fix an arbitrary $\varepsilon > 0$ and consider $\varepsilon/2$ -neighborhood $O_\varepsilon(\Delta)$ of Δ . According to the basic properties of convergent sequences, $O(\Delta)$ contains all the terms of the sequences $\{S(M_n^{\text{ext}})\}$ and $\{S(M_n^{\text{int}})\}$ starting from some number k . The difference of any two numbers which are taken from $O_{\varepsilon/2}(\Delta)$ is less than ε , then

$S(M_n^{\text{ext}}) - S(M_n^{\text{int}}) < \varepsilon$. For any concrete $\bar{n} > k$ we have two measurable figures $M_{\bar{n}}^{\text{int}}, M_{\bar{n}}^{\text{ext}}$ such that $M_{\bar{n}}^{\text{int}} \subset \Omega \subset M_{\bar{n}}^{\text{ext}}$ and $S(M_{\bar{n}}^{\text{ext}}) - S(M_{\bar{n}}^{\text{int}}) < \varepsilon$. And ε can be fixed from the very beginning as an arbitrary small positive number, then (assertion4) Ω is measurable and the number $S(\Omega)$ is defined. Next, from $M_n^{\text{int}} \subset \Omega \subset M_n^{\text{ext}} (\forall n)$ (auxiliary1) follows that

$S(M_n^{\text{int}}) \leq S(\Omega) \leq S(M_n^{\text{ext}}) (\forall n)$ [T], both sequences $\{S(M_n^{\text{int}})\}$ and $\{S(M_n^{\text{ext}})\}$ go to the same limit, we can consider the stationary sequence $\{x_n\} \equiv S(\Omega), S(\Omega), S(\Omega), \dots$ and apply the squeeze theorem for sequences in [T], then $S(\Omega)$ is equal to $\lim_{n \rightarrow \infty} S(M_n^{\text{int}}) = \lim_{n \rightarrow \infty} S(M_n^{\text{ext}})$.

Assertion6. For any real number a there exist a monotonically increasing sequence of rational numbers $\left\{ \frac{m_n}{10^n} \right\} \rightarrow a$ (here $n = 1, 2, 3, 4, \dots$ and $m_1, m_2, m_3, m_4, \dots$ are integer numbers)

and a monotonically decreasing sequence of rational numbers $a \leftarrow \left\{ \frac{\bar{m}_n}{10^n} \right\}$.

Proof. Let's take the decimal notation of $a = \pm \partial_1 \partial_2 \dots \partial_n, d_1 d_2 d_3 \dots$. Let a is not negative ($a \geq 0$): $a = \partial_1 \partial_2 \dots \partial_n, d_1 d_2 d_3 \dots$. We can take the sequence:

$$q_1 = \partial_1 \partial_2 \dots \partial_n, d_1 00000 \dots \parallel q_2 = \partial_1 \partial_2 \dots \partial_n, d_1 d_2 0000 \dots$$

$$\parallel q_3 = \partial_1 \partial_2 \dots \partial_n, d_1 d_2 d_3 000 \dots \parallel q_4 = \partial_1 \partial_2 \dots \partial_n, d_1 d_2 d_3 d_4 00 \dots \text{ and etc.}$$

This sequence is monotonically increasing and it goes to a . The term q_1 can be represented as

$$\left\{ \frac{m_1}{10^1} \right\} \parallel m_1 \in \mathbb{Z}, \text{ the term } q_2 \text{ can be represented as } \left\{ \frac{m_2}{10^2} \right\} \parallel m_2 \in \mathbb{Z}, \text{ the term } q_3 \text{ can be represented}$$

$$\text{as } \left\{ \frac{m_3}{10^3} \right\} \parallel m_3 \in \mathbb{Z} \text{ and etc. So we have a monotonically increasing sequence } \left\{ \frac{m_n}{10^n} \right\} \rightarrow a.$$

Let's build the second sequence. Again $a = \partial_1 \partial_2 \dots \partial_n, d_1 d_2 d_3 \dots$ and we take

$$\bar{q}_1 = \partial_1 \partial_2 \dots \partial_n, d_1 00000 \dots + \frac{1}{10} \parallel \bar{q}_2 = \partial_1 \partial_2 \dots \partial_n, d_1 d_2 0000 \dots + \frac{1}{10^2} \parallel$$

$$\parallel \bar{q}_3 = \partial_1 \partial_2 \dots \partial_n, d_1 d_2 d_3 000 \dots + \frac{1}{10^3} \dots \parallel \bar{q}_4 = \partial_1 \partial_2 \dots \partial_n, d_1 d_2 d_3 d_4 000 \dots + \frac{1}{10^4} \text{ and etc.}$$

This sequence is monotonically decreasing and it goes to a . And here again, the term q_1 can be

$$\text{represented as } \left\{ \frac{\bar{m}_1}{10^1} \right\} \parallel \bar{m}_1 \in \mathbb{Z}, \text{ the term } q_2 \text{ can be represented as } \left\{ \frac{\bar{m}_2}{10^2} \right\} \parallel \bar{m}_2 \in \mathbb{Z}, \text{ the term } q_3 \text{ can}$$

$$\text{be represented as } \left\{ \frac{\bar{m}_3}{10^3} \right\} \parallel \bar{m}_3 \in \mathbb{Z} \text{ and etc. So we have a monotonically decreasing sequence}$$

$$\left\{ \frac{\bar{m}_n}{10^n} \right\} \rightarrow a. \text{ Let now } -a \text{ is a negative real number } (-a < 0), \text{ so } -a = -\partial_1 \partial_2 \dots \partial_n, d_1 d_2 d_3 \dots$$

Let's take the positive number $a = \partial_1 \partial_2 \dots \partial_n, d_1 d_2 d_3 \dots$ (we reflect a over the zero) and we build

two sequences that we need, for the positive number a . Then we reflect everything back over the zero (instead of each sequence we will have an opposite to it). A decreasing sequence (after reflection) will become an increasing sequence which goes to $-a$, and an increasing sequence (after reflection) will become a decreasing sequence which goes to $-a$.

$$\text{And finally, when } a = 0 \text{ we can take the sequences } \left\{ \frac{-1}{10^n} \right\}, \left\{ \frac{1}{10^n} \right\}.$$

Let's prove now **the main theorem**.

The area of any rectangle, which sides a, b are parallel to coordinate axes, equals $a \cdot b$.

We fix any Π on the plane with sides a, b . We can chose it's vertex which x -coordinate and y -coordinate are both minimal, let it be (x_0, y_0) .

Then $(x_0 + a, y_0)$, $(x_0, y_0 + b)$, $(x_0 + a, y_0 + b)$ - coordinates of other vertexes.

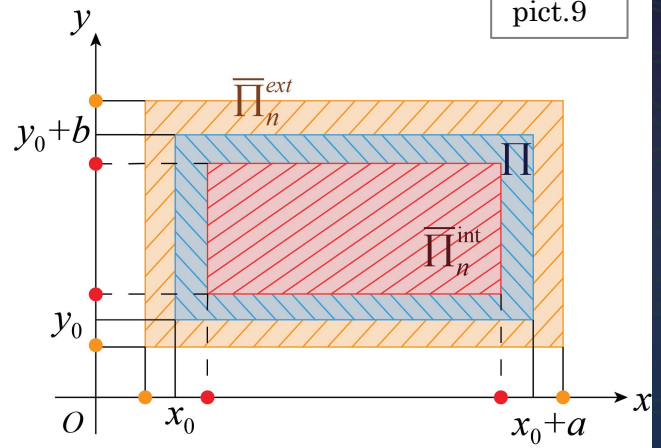
For each coordinate of each vertex ([assertion6](#)) we build two monotonic sequences which converge to that coordinate. For any concrete number $n \in \mathbb{N}$ we can mark the terms of these sequences which belong to the segments $[x_0, x_0 + a]$, $[y_0, y_0 + b]$, red points **[pict9]** (for any $n \in \mathbb{N}$ there are 4

terms) these terms define an internal rectangle $\bar{\Pi}_n^{\text{int}}$ (red) which coordinates are like in the [assertion3](#), then $\bar{\Pi}_n^{\text{int}}$ is measurable and we know it's area.

Next, for any $n \in \mathbb{N}$ we can mark the terms of the sequences which do not belong to the intervals $(x_0, x_0 + a)$, $(y_0, y_0 + b)$, orange points [\[pict9\]](#)

(for any $n \in \mathbb{N}$ there are 4 terms). These terms define an external rectangle $\bar{\Pi}_n^{\text{ext}}$ (orange) which coordinates are like in the [assertion3](#), then $\bar{\Pi}_n^{\text{ext}}$ is measurable and

we know it's area. The sides of $\{\bar{\Pi}_n^{\text{int}}\}$, which are parallel to Ox , form a sequence that goes to a . Really, the sequence of the “right ends” goes to $x_0 + a$, the sequence of the “left ends” goes to x_0 , then their difference (which is always a length of a side) goes to a . The sides of $\bar{\Pi}_n^{\text{int}}$, which are parallel to Oy , form a sequence that goes to b . Then the sequence of areas $\{S(\bar{\Pi}_n^{\text{int}})\}$ goes to $a \cdot b$. And similarly, the sequence of external areas $\{S(\bar{\Pi}_n^{\text{ext}})\}$ goes to $a \cdot b$. Then, according to the [assertion5](#), Π is measurable and $S(\Pi) = a \cdot b$. Everything is proved.



From the [main theorem](#) immediately follows the property [\[1\]](#) of area:

the area of any unit square 1×1 , which sides are parallel to coordinate axes, is equal to 1.

Let's finally prove the [\[3\]](#)-rd property of area (equal measurable figures have equal areas).

Let Ω and Ψ are equal figures, according to the [def2](#), there exist one-to-one correspondence $f: \Omega \rightarrow \Psi$ which conserves distances and parallelism. As Ω is measurable, we have

$\lim_{n \rightarrow \infty} S(\Omega_n^{\text{ext}}) = \lim_{n \rightarrow \infty} S(\Omega_n^{\text{int}}) = S(\Omega)$ [\[B1\]](#). And for any concrete $n \in \mathbb{N}$ we have

$\Omega_n^{\text{int}} \subset \Omega \subset \Omega_n^{\text{ext}}$. Then for the images of these figures we have

$f(\Omega_n^{\text{int}}) \subset f(\Omega) \subset f(\Omega_n^{\text{ext}}) \Leftrightarrow // \text{ as } f(\Omega) = \Psi // \Leftrightarrow f(\Omega_n^{\text{int}}) \subset \Psi \subset f(\Omega_n^{\text{ext}})$ [\[B2\]](#).

The figure Ω_n^{int} consists of T_n net squares, the sides of each square are parallel to coordinate axes and both sides are equal to 10^{-n} . We know that f conserves distances and parallelism, so f translates every net-square into the equal square, which sides are still parallel to coordinate axes, and are still 10^{-n} each, then, by the [theorem4](#), the area of such square is 10^{-2n} (the same as it was).

The figure Ω_n^{int} consists of T_n squares without common internal points, then the image $f(\Omega_n^{\text{int}})$ also consists of T_n squares without common internal points. Then, by additivity [\[2\]](#),

$S(f(\Omega_n^{\text{int}})) = T_n \cdot 10^{-2n}$ and $S(\Omega_n^{\text{int}}) = T_n \cdot 10^{-2n}$. So, for any n we have $S(\Omega_n^{\text{int}}) = S(f(\Omega_n^{\text{int}}))$ and similarly $S(\Omega_n^{\text{ext}}) = S(f(\Omega_n^{\text{ext}}))$. Then, the sequences $\{S(f(\Omega_n^{\text{int}}))\}$ and $\{S(f(\Omega_n^{\text{ext}}))\}$ coincide with the sequences $\{S(\Omega_n^{\text{int}})\}$ and $\{S(\Omega_n^{\text{ext}})\}$, therefore they both go to the same limit $\{S(\Omega)\}$.

As we noticed above, for any $n \in \mathbb{N}$ we have $f(\Omega_n^{\text{int}}) \subset f(\Omega) \subset f(\Omega_n^{\text{ext}})$. We know that $\lim S(f(\Omega_n^{\text{int}})) = \lim S(f(\Omega_n^{\text{ext}})) = S(\Omega)$, then from the [assertion5](#) follows that $f(\Omega)$ is measurable and $S(f(\Omega)) = S(\Omega)$. We have proved the properties [1],[3] of area. The additivity [2] was proved in the [assertion2](#). The existence of area is proved.

The proof of the **uniqueness of area** is very simple, but we are lack of just one additional auxiliary fact: if figures Ω and Ψ are measurable, then the figure $\Omega \setminus \Psi$ is also measurable. If we have this fact, then the proof of the uniqueness can be performed very quickly. But now it's not clear how to obtain this result from the results that we have above. In order to prove this one we need to introduce the last measurability criterion. By using it, we will be able to get the needed result and to prove the uniqueness. Also the last **[3-rd criterion of measurability]** has a great importance in math.

Def: a figure X is called a zero area figure if it's area is zero, $S(X) = 0$.

It's very easy to understand that for any zero area figure: any internal figure X_k^{int} is an empty figure. Really, if we assume that there is some net-square in X_k^{int} then the area $S(X_k^{\text{int}})$ is a positive number. For any figure, the sequence of areas of internal figures is monotonically increasing: $S(X_k^{\text{int}}) \leq S(X_{k+1}^{\text{int}}) \leq S(X_{k+2}^{\text{int}}) \leq \dots$, then starting from the number k all the terms of the sequence $\{S(X_n^{\text{int}})\}$ are greater than the fixed positive number $S(X_k^{\text{int}})$, then $\{S(X_n^{\text{int}})\}$ can't converge to zero and $S(X) \neq 0$, and we have a contradiction. So, any internal figure X_k^{int} is an empty figure, it doesn't contain any squares at all, i.e., $T_n = 0 \quad \forall n \in \mathbb{N}$, then $T_n \cdot 10^{-2n} = S(X_n^{\text{int}}) = 0 \quad \forall n \in \mathbb{N}$.

And what about external figures X_n^{ext} ? These figures already contain some squares, and the sequence $S(X_n^{\text{ext}})$ is monotonically decreasing (this sequence is decreasing for any bounded figure, not only for X) and goes to zero: $\{S(X_n^{\text{ext}})\} \rightarrow 0$.

[Assertion7](#). A union $P \cup X$ of any zero-area figures P and X is again a zero-area figure.

Proof. Let P and X are zero-area figures. For any $n \in \mathbb{N}$ we obviously have

$(P \cup X)_n^{\text{ext}} \subset P_n^{\text{ext}} \cup X_n^{\text{ext}}$ [L]. Then $S((P \cup X)_n^{\text{ext}}) \leq S(P_n^{\text{ext}}) + S(X_n^{\text{ext}})$. Both sequences $\{S(P_n^{\text{ext}})\}$ and $\{S(X_n^{\text{ext}})\}$ go to zero, then $\{S((P \cup X)_n^{\text{ext}})\}$ also goes to zero. So, the sequence of areas of external quadratic figures for $P \cup X$ goes to zero, then $S(P \cup X) = 0$.

[Assertion8](#). Any part of a zero-area figure is again a zero-area figure, i.e., $S(P) = 0$ and $X \subset P$, then $S(X) = 0$.

Proof. Obviously $X_n^{\text{ext}} \subset P_n^{\text{ext}}$, then $S(X_n^{\text{ext}}) \leq S(P_n^{\text{ext}})$. From $\{S(P_n^{\text{ext}})\} \xrightarrow{n \rightarrow \infty} 0$ follows that $\{S(X_n^{\text{ext}})\} \xrightarrow{n \rightarrow \infty} 0$.

Assertion9. Ω is a plane figure (or a space figure). Any segment AB which connects an internal point A (of Ω) and an external point B (of Ω) contains at least one boundary point of Ω .

Proof. Without loss of generality, let Ω is some plane figure. Let's fix any internal point A and any external point B . Let's draw the coordinate line L through

A and B such that A is a point with a zero coordinate, and the segment AB lies on the positive ray of L .

Let's consider all the internal points of Ω which lie on L , this set is not empty (at least it contains A), coordinates of these points form some set \tilde{R} of real numbers, this set is bounded above, by the coordinate b of B . Then \tilde{R} has a supremum h which can be pictured as a point H , let's

show that H is a boundary point of Ω [pict10]. If we assume that H is an internal/external point of Ω , then it has the neighborhood $O_\varepsilon(H)$ which (completely belongs to Ω)/(does not have any common points with Ω), then the interval $O_\varepsilon(H) \cap L$ on L (completely belongs to Ω)/(does not have any common points with Ω). Then there is an interval of real numbers with the center at h which (belongs to \tilde{R})/(does not have any common points with \tilde{R}), in both cases h is not a supremum of \tilde{R} . Then H is a boundary point of Ω .

Consequence2. Any segment AB which connects any point $A \in \Omega$ and any point $B \notin \Omega$, contains at least one boundary point of Ω .

Proof. $A \in \Omega$ then there can be only two variants: A is a boundary point of Ω , or A is an internal point of Ω . If A is a boundary point, then AB contains the boundary point A . Let A is an internal point (of Ω). We know that $B \notin \Omega$, then there are exactly two variants: B is a boundary point of Ω (then AB contains the boundary point B), or B is an external point (of Ω), then, according to the [assertion9](#), AB contains some boundary point. Everything is proved.

Assertion10 [3-rd criterion of measurability].

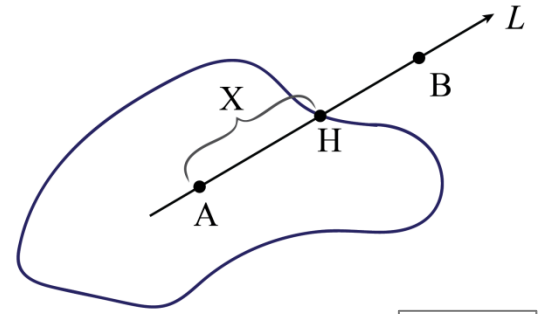
Ω is measurable \Leftrightarrow the boundary $\partial\Omega$ is a zero-area figure.

Proof. \Rightarrow Let Ω is measurable, we need to show that

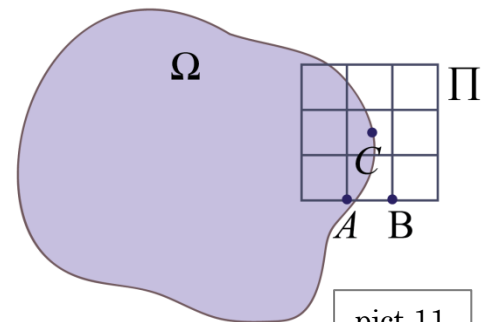
$S(\partial\Omega) = 0$. Let's fix any $n \in \mathbb{N}$ and a quadratic net for n .

We fix any net-square which has a common point C with $\partial\Omega$

[pict11] (it is a square from $(\partial\Omega)_n^{ext}$), this square has exactly 8 neighbor-squares around. All these 9 squares together form a bigger square Π . As C belongs to the center-square, we can draw a small neighborhood $O_\varepsilon(C)$ which belongs to Π , this



pict.10



pict.11

neighborhood must contain one point $A \in \Omega$ and one point $B \notin \Omega$ (because C is a boundary point). Then the big square Π contains at least one point A from Ω and one point B not from Ω . Let's show that some small square (one of the 9 squares that form Π) has the same property. Here is a simple logic: any small square may **[A]** have a common point with Ω , but do not belong to Ω completely **[B]** belong to Ω **[C]** do not have any common points with Ω .

If some small square is such that **[A]**, then it has the same property as Π (contains one point from Ω and one not from Ω). Let's assume that there is no such small square, so every small square is such that **[B]** or **[C]**. All 9 small squares can't be such that **[B]**, because then Π does not contain any point not from Ω . And similarly, all 9 small squares can't be such that **[C]**, because then Π does not contain any point from Ω . And **what if** some of these 9 squares completely belong to Ω , and the others do not have any common points with Ω ? In such case there will be two small neighbor-squares with a common side, such that one square completely belongs to Ω , and the other one has no common points with Ω , so the common side of these squares belongs and doesn't belong to Ω at the same time, and we have a contradiction.

Then there exist some small square (among these 9 squares) such that **[A]**. This small square contains some point $A \in \Omega$ and therefore it belongs to Ω_n^{ext} , and it also contains some point $B \notin \Omega$, then it does not belong to Ω_n^{int} . So that square belongs to $\Omega_n^{ext} \setminus \Omega_n^{int}$.

Let's sum up: we had started from any square ∂ from $(\partial\Omega)_n^{ext}$, and we deduced that the square ∂ , or one of 8 squares around ∂ belongs to $\Omega_n^{ext} \setminus \Omega_n^{int}$. Let's estimate from above the number of squares in $(\partial\Omega)_n^{ext}$. The most convenient way to do it is to build the correspondence

$$f : (\partial\Omega)_n^{ext} \rightarrow \Omega_n^{ext} \setminus \Omega_n^{int}.$$

For any concrete square ∂ from $(\partial\Omega)_n^{ext}$ we define $f(\partial) = \rho \in \Omega_n^{ext} \setminus \Omega_n^{int}$, where ρ is the square from $\Omega_n^{ext} \setminus \Omega_n^{int}$ (here $\rho = \partial$ or ρ is one of 8 squares around ∂).

Then some of the squares of the figure $\Omega_n^{ext} \setminus \Omega_n^{int}$ correspond to the squares of $(\partial\Omega)_n^{ext}$.

There are exactly $H_n(\text{for } \Omega) - T_n(\text{for } \Omega)$ different squares in $\Omega_n^{ext} \setminus \Omega_n^{int}$ and any square may correspond maximum to 9 squares (to itself and to every of 8 surrounding squares), so $9 \cdot (H_n(\text{for } \Omega) - T_n(\text{for } \Omega))$ is the maximal number of squares that can correspond to the squares of $\Omega_n^{ext} \setminus \Omega_n^{int}$, then there can't be more than $9 \cdot (H_n(\text{for } \Omega) - T_n(\text{for } \Omega))$ squares in the figure $(\partial\Omega)_n^{ext}$. Let's write it: $H_n(\text{for } \partial\Omega) \leq 9 \cdot (H_n(\text{for } \Omega) - T_n(\text{for } \Omega))$ let's multiply both sides by 10^{-2n} , we will get $S((\partial\Omega)_n^{ext}) \leq 9 \cdot (S(\Omega_n^{ext}) - S(\Omega_n^{int}))$. When $n \rightarrow \infty$ the right part of the last equality goes to zero (because Ω is measurable), then $S((\partial\Omega)_n^{ext}) \xrightarrow{n \rightarrow \infty} 0$ then $S(\partial\Omega) = 0$.

Conversely. \Leftarrow (More simple). Let $\partial\Omega$ is a zero-area figure. Let's take any net-square δ which has a common point with Ω , but does not belong to Ω completely, it is a square from $\Omega_n^{ext} \setminus \Omega_n^{int}$. That δ contains some point $A \in \Omega$ and some point $B \notin \Omega$, the segment AB belongs to δ and (consequence from [assertion9](#)) contains a boundary point $C \in \partial\Omega$. Then δ belongs to $(\partial\Omega)_n^{ext}$. Therefore, any square from $\Omega_n^{ext} \setminus \Omega_n^{int}$ is a square from $(\partial\Omega)_n^{ext}$, so we have $\Omega_n^{ext} \setminus \Omega_n^{int} \subset (\partial\Omega)_n^{ext}$. Then the number of squares in $\Omega_n^{ext} \setminus \Omega_n^{int}$ is not greater than the number of squares in $(\partial\Omega)_n^{ext}$. Let's write it: $H_n(for\Omega) - T_n(for\Omega) \leq H_n(for\partial\Omega)$, we multiply both sides by 10^{-2n} , then $S(\Omega_n^{ext}) - S(\Omega_n^{int}) \leq S((\partial\Omega)_n^{ext})$. When $n \rightarrow \infty$ the right part goes to zero, then the left part also goes to zero and Ω is measurable.

Consequence3. If Ω, Ψ are measurable figures, then $\Omega \setminus \Psi$ is also a measurable figure.

The main idea: As Ω, Ψ are measurable, then their boundaries $\partial\Omega, \partial\Psi$ are zero-area figures ([assertion10](#)), then $\partial\Omega \cup \partial\Psi$ is a zero area figure ([assertion7](#)).

We will show that the boundary $\partial(\Omega \setminus \Psi)$ of the figure $\Omega \setminus \Psi$ belongs to $\partial\Omega \cup \partial\Psi$, i.e., $\partial(\Omega \setminus \Psi) \subset \partial\Omega \cup \partial\Psi$, then ([assertion8](#)) the boundary $\partial(\Omega \setminus \Psi)$ is a zero-area figure.

Then ([assertion10](#)) $\Omega \setminus \Psi$ is measurable.

So we just have to show that $\partial(\Omega \setminus \Psi) \subset \partial\Omega \cup \partial\Psi$ and the case is done.

Let's define: for any figure Ω on the plane Π , the figure $\Pi \setminus \Omega \equiv \Omega^C$ is called a complement of Ω .

[Fact 1] for any figures Ω, Ψ we have $\Omega \setminus \Psi = \Omega \cap \Psi^C$ (this one is very simple, we just need to write what kind of points belong to $\Omega \setminus \Psi$, and what kind of points belong to $\Omega \cap \Psi^C$. We will see that these are exactly the same points).

[Fact 2] Any figure Ω and it's complement Ω^C always have a common boundary, i.e., $\partial\Omega = \partial\Omega^C$ (just use the definition of a boundary point and show that $\partial\Omega \subset \partial\Omega^C$ and $\partial\Omega^C \subset \partial\Omega$).

[Fact 3] for any figures Ω, Ψ we have $\partial(\Omega \cap \Psi) \subset \partial\Omega \cup \partial\Psi$

(here we need to fix any boundary point A of $\Omega \cap \Psi$, and it's very easy to deduce that this point may be: a boundary point of Ω , or a boundary point of Ψ , or a boundary point of Ω and a boundary point of Ψ , so in any case, A belongs to the union $\partial\Omega \cup \partial\Psi$, from here follows $\partial(\Omega \cap \Psi) \subset \partial\Omega \cup \partial\Psi$)

We are ready to prove [Y]: $[Fact 1] \Omega \setminus \Psi = \Omega \cap (\Psi^C) \Rightarrow \partial(\Omega \setminus \Psi) = \partial(\Omega \cap (\Psi^C)) \Rightarrow \Rightarrow [Fact 3]: \partial(\Omega \setminus \Psi) \subset \partial\Omega \cup \partial\Psi^C \Rightarrow [Fact 2]: \partial(\Omega \setminus \Psi) \subset \partial\Omega \cup \partial\Psi$. And [T] is proved.

We are ready to prove the uniqueness of area.

Uniqueness of area. Let there exist some correspondence \tilde{S} which is defined on the collection of all measurable figures ([def4](#)) and satisfies to [1],[2],[3], then $\tilde{S} \equiv S$. The proof here is simple,

let's describe the main steps. For any 1×1 square: $\tilde{S}(1 \times 1) = 1$ (according to [1]). We can draw several parallel lines in order to divide 1×1 square into n^2 equal small squares with sides $1/n$ each. As [1] $\tilde{S}(1 \times 1) = 1$, then by additivity, the area of any $1/n \times 1/n$ square is $1/n^2$ (and it is true for any $n \in \mathbb{N}$).

Let now Ω is any measurable figure.

If $P \subset \Omega$, then $\tilde{S}(P) \leq \tilde{S}(\Omega)$ [monotonicity]. Really, let $P \subset \Omega$ are measurable figures, then $\Omega \setminus P$ is measurable (consequence3). And we have $P \cup \Omega \setminus P = \Omega$, where figures P and $\Omega \setminus P$ do not have any common internal points, then by additivity [2]: $\tilde{S}(P) + \tilde{S}(\Omega \setminus P) = \tilde{S}(\Omega) \Rightarrow \tilde{S}(P) \leq \tilde{S}(\Omega)$.

Next: as \tilde{S} coincides with S on every $1/n \times 1/n$ square, then (by additivity [2]), \tilde{S} coincides with S on every figure Ω_n^{int} and Ω_n^{ext} . As Ω is measurable, we have

$\lim_{n \rightarrow \infty} S(\Omega_n^{\text{int}}) = \lim_{n \rightarrow \infty} S(\Omega_n^{\text{ext}}) = S(\Omega)$, then we have:

[U] $\lim_{n \rightarrow \infty} \tilde{S}(\Omega_n^{\text{int}}) = \lim_{n \rightarrow \infty} \tilde{S}(\Omega_n^{\text{ext}}) = S(\Omega)$. So, the sequences $\{\tilde{S}(\Omega_n^{\text{int}})\}$ and $\{\tilde{S}(\Omega_n^{\text{ext}})\}$ go to the same limit $S(\Omega)$. In the same time for any n we have $\Omega_n^{\text{int}} \subset \Omega \subset \Omega_n^{\text{ext}} \Rightarrow$ [monotonicity] $\Rightarrow \tilde{S}(\Omega_n^{\text{int}}) \leq \tilde{S}(\Omega) \leq \tilde{S}(\Omega_n^{\text{ext}})$ and here we can use the **squeeze theorem for sequences** $\{\tilde{S}(\Omega_n^{\text{int}})\}$ and $\{\tilde{S}(\Omega_n^{\text{ext}})\}$ and $\{\tilde{S}(\Omega)\} = \tilde{S}(\Omega), \tilde{S}(\Omega), \tilde{S}(\Omega), \tilde{S}(\Omega), \dots$

Both sequences $\{\tilde{S}(\Omega_n^{\text{int}})\}$ and $\{\tilde{S}(\Omega_n^{\text{ext}})\}$ **[U]** go to the same limit $S(\Omega)$, then $\{\tilde{S}(\Omega)\}$ goes to the same limit, therefore $S(\Omega) = \tilde{S}(\Omega)$. So \tilde{S} coincides with S on every measurable figure Ω , it means that $S \equiv \tilde{S}$ and the area is unique.

The definition of a volume V and it's properties (including uniqueness) are exactly similar.

Moreover, the construction process and the theorems (including **criteria of measurability 1,2,3**) are also exactly similar.

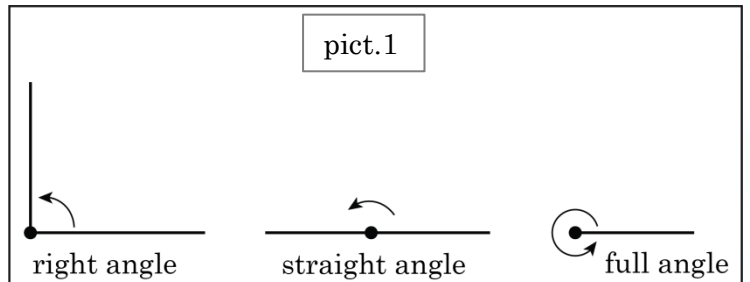
9

Angles

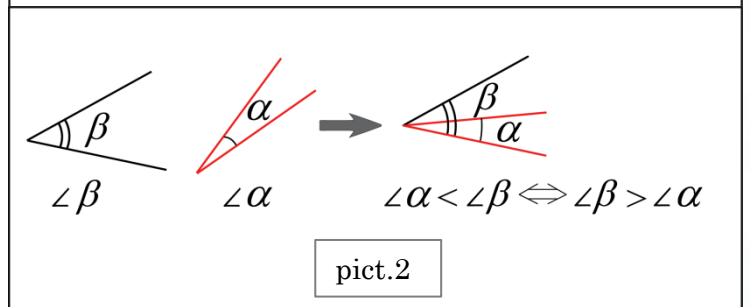
Angles

When we speak about points, lines, rays, segments (on the plane or in the space) we do not define these objects, because for us these are basic “elementary” objects. Both plane geometry and stereometry have it’s own axioms and basic objects like “planes”, “lines” and etc. (in fact the plane geometry is a part of stereometry). Basic geometrical axioms and theorems is an independent part of mathematics, it does not depend on the theory of real numbers.

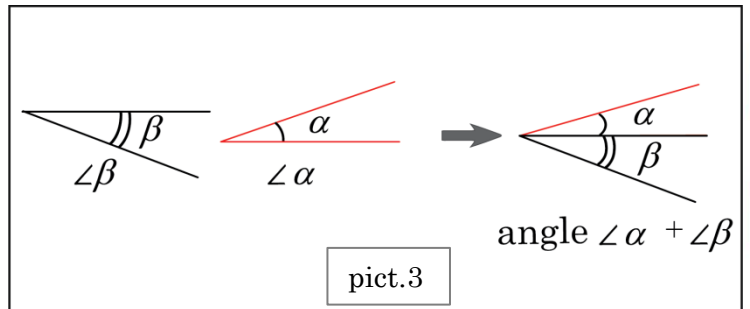
One of the basic geometrical figures is the angle $\angle BOA$, it is a figure which consists of two rays OB and OA and the part of the plane, which lies “between” these rays. In any particular case we have to show which part of the plane between OB and OA is a part of our angle (because there is always two variants). The point O is called a “vertex of the angle”. Our basic angles are: the right angle $\angle(\text{right angle})$, the straight angle $\angle(\text{straight angle})$ and the full angle $\angle(\text{full angle})$ [pict1].



We can compare angles [pict2] in the similar way as we compare segments. The writings $\angle\alpha < \angle\beta$ and $\angle\beta > \angle\alpha$ are equivalent.



We can add any two angles $\angle\alpha$ and $\angle\beta$ if they are both are less than the straight angle [pict3], the result angle is called a “sum of angles α and β ” and we denote it $\angle(\alpha + \beta)$.



For any angle $\angle\alpha$:

$$\angle\alpha + \dots + \angle\alpha \equiv [n \text{ summands}] \equiv \angle n\alpha, \text{ this}$$

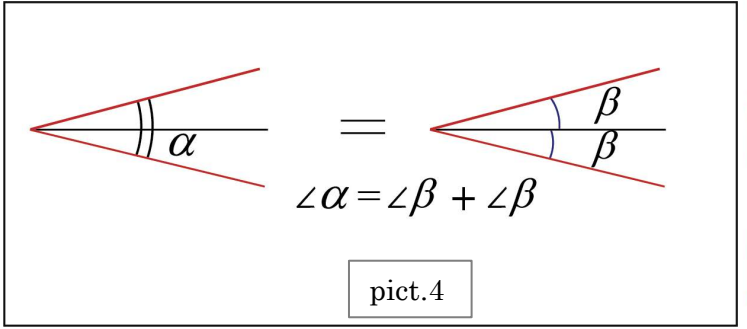
definition is correct only for such numbers n , for which the sum $\angle\alpha + \dots + \angle\alpha$ is less than the full angle. It’s easy to see that:

$$\angle(\text{straight angle}) = \angle 2(\text{right angle})$$

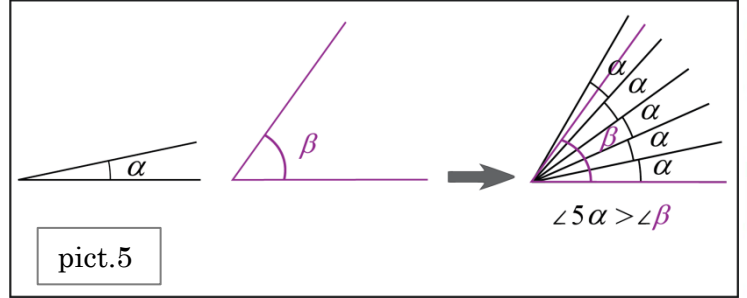
$$\text{and } \angle(\text{full}) = \angle 4(\text{right angle}).$$

If we have $\angle n\beta = \angle\alpha$, then we can write $\angle\beta \equiv \angle(\alpha/n)$.

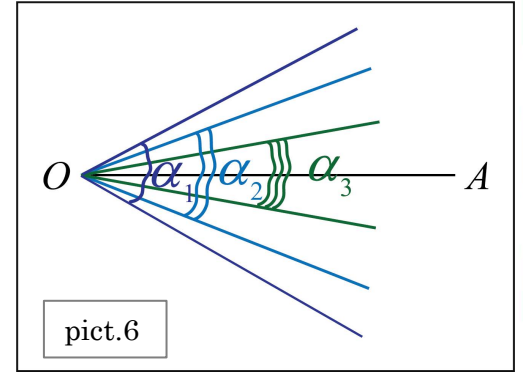
Half angle assumption. For any angle $\angle\alpha$ there exist the angle $\angle\beta$ such that $\angle\beta = \angle(\alpha/2)$ [pict4]. We also assume that the right angle $\angle(\text{right angle})$ can be divided into 90 equal parts, so there exist “the unit angle” $\angle e$ such that $\angle(\text{right angle}) = \angle 90e$.



Archimedes axiom. For any angles $\angle\alpha$ and $\angle\beta$ (where $\angle\alpha < \angle(\text{straight angle})$ and $\angle\beta < \angle(\text{straight angle})$) there exist some natural n such that $\angle n\alpha > \angle\beta$. [pict5].



Nested angles axiom. If we have some sequence $\{\angle\alpha_n\}$ of nested angles: $\angle\alpha_1 \supset \angle\alpha_2 \supset \angle\alpha_3 \supset \dots$, with a common vertex O , then there exist the ray OA , which belongs to every angle $\angle\alpha_n \parallel \forall n$ [pict6].



Def. $\Omega \equiv \{\angle\alpha \mid \angle\alpha < \angle(\text{full angle})\}$. The “Angle value” is the correspondence $L: \Omega \rightarrow R^+$ which compares only one non-negative real number $L(\angle\alpha)$ for every angle $\angle\alpha$. And also:

[1] $L(\angle e) = 1$ [2] for any angles $\angle\alpha$ and $\angle\beta$ (where $\angle\alpha < \angle(\text{straight angle})$ and $\angle\beta < \angle(\text{straight angle})$) we have: $L(\angle\alpha + \angle\beta) = L(\angle\alpha) + L(\angle\beta)$.

[3] If $\angle\alpha = \angle\beta$, then $L(\angle\alpha) = L(\angle\beta)$.

For any angle $\angle\alpha$, the number $L(\angle\alpha)$ is called a value of the angle $\angle\alpha$.

The construction of the angle value L is very similar to the length construction.

For any angle $\angle\alpha$ the number $L(\angle\alpha)$ is usually written with the “degree symbol” $^\circ$ right after it.

Like $L(\angle e) = 1^\circ$, $L(\angle \text{right angle}) = 90^\circ$, $L(\angle \text{straight angle}) = 180^\circ$. In practice we never say “the value of the angle $\angle\alpha$ is one degree”, but only “ $\angle\alpha$ is one degree”.

Property. $\angle\alpha > \angle\beta \Leftrightarrow L(\angle\alpha) > L(\angle\beta)$. And for any real number $a \in [0^\circ, 360^\circ]$ there exist the angle $\angle\alpha$ such that $L(\angle\alpha) = a$.

Def1. Any angle, which is less than the right angle, is called an “acute angle”.

An angle $\angle\alpha$ is acute if and only if $L(\angle\alpha) \in [0^\circ, 90^\circ)$. Any angle, which is greater than the right angle and less than the straight angle, is called an “obtuse angle”. An angle $\angle\beta$ is obtuse if and only if $L(\angle\beta) \in (90^\circ, 180^\circ)$. In practice we neglect the letter L and the symbol \angle , instead of $L(\angle\alpha) = 50^\circ$ we write just $\alpha = 50^\circ$, instead of $L(\angle\beta) = 30^\circ$ we write $\beta = 30^\circ$.

Trigonometric functions. In the course of plane geometry basic trigonometric functions \sin, \cos, tg, ctg are defined for any **acute** angle α through the right triangle. We just need to draw any right triangle with an angle α and calculate a ratio of relevant sides.

This definition is correct, because all the right triangles with the same angle α are similar, and the ratio of relevant sides in any triangle is always the same. For any acute angle α the main

values are $\sin \alpha$ and $\cos \alpha$, because $tg \alpha = \frac{\sin \alpha}{\cos \alpha}$, $ctg \alpha = \frac{\cos \alpha}{\sin \alpha}$.

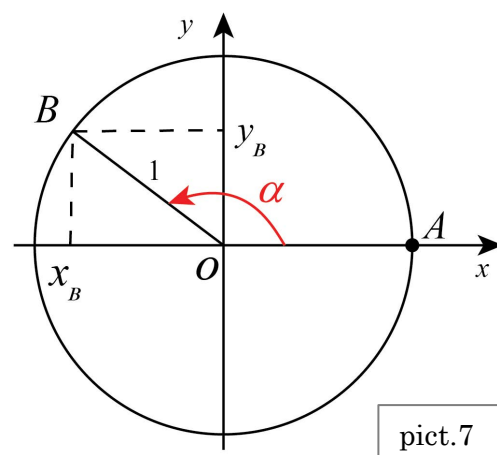
By using simple ideas from elementary geometry we can build the small table:

– / –	30°	45°	60°
\sin	$1/2$	$1/\sqrt{2}$	$\sqrt{3}/2$
\cos	$\sqrt{3}/2$	$1/\sqrt{2}$	$1/2$
tg	$1/\sqrt{3}$	1	$\sqrt{3}$
ctg	$\sqrt{3}$	1	$1/\sqrt{3}$

Let's extend the notion of angle and trigonometric functions.

We fix any coordinate system Oxy and draw the unit circle with the center at the origin. We also mark the point A , at which Ox intersects the circle.

Let's take any angle $\alpha \in [0^\circ, 360^\circ]$. By moving along the circle from the point A in the **counterclockwise direction** we build the angle $\angle AOB = \angle \alpha$ [pict7], the point B has some coordinates x_B and y_B , then we define:



pict.7

$\cos \alpha \equiv // \text{by definition} // \equiv x_B \parallel \sin \alpha \equiv y_B \parallel tg \alpha \equiv \frac{\sin \alpha}{\cos \alpha} \parallel ctg \alpha \equiv \frac{\cos \alpha}{\sin \alpha} \parallel$.

It's very important to notice that this definition of trigonometric functions \sin, \cos, tg, ctg extends the old definition, where trigonometric functions are defined only for acute angles.

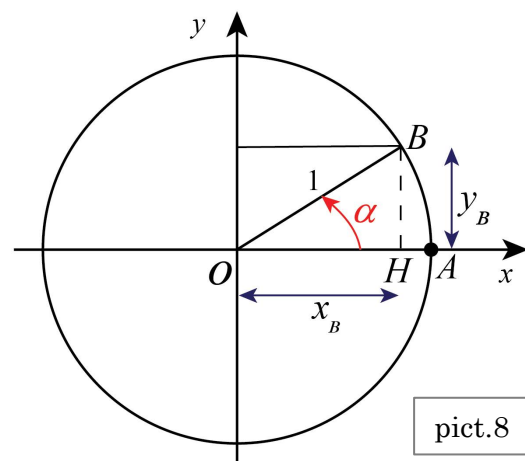
Really, let's take any acute angle α and build the angle $\angle AOB = \angle \alpha$, then we can draw $BH \perp Ox$. We will get the right triangle, which hypotenuse OB is 1.

The numbers x_B and y_B are coordinates of the point B , but in the same time these numbers are cathetuses of the right triangle $\triangle OBH$ [pict8].

So, according to the old definition:

$$\frac{y_B}{1} = \sin \alpha = y_B \text{ and } \frac{x_B}{1} = \cos \alpha = x_B.$$

Then the new definition is really an extension of the old one.



Next, the function $tg \alpha$ is not defined when $\cos \alpha = 0$ (when $\alpha = 90^\circ$ or $\alpha = 270^\circ$), and $ctg \alpha$ is not defined when $\sin \alpha = 0$ (when $\alpha = 0^\circ$ or $\alpha = 180^\circ$).

For any angle α , the values $\sin \alpha$ and $\cos \alpha$ are numbers from the segment $[-1, 1]$, the only restriction is: $\sin^2 \alpha + \cos^2 \alpha = 1$. Really, any angle $\angle \alpha \in [0^\circ, 360^\circ]$ defines some point B on the circle such that $\angle \alpha = \angle AOB$, and for any point B on the unit circle we obviously have $x_B^2 + y_B^2 = 1 \Leftrightarrow \sin^2 \alpha + \cos^2 \alpha = 1$ it follows from the Pythagorean theorem for the right triangle with sides $|x_B|$, $|y_B|$, 1. The values of $tg \alpha$ and $ctg \alpha$ can be any real numbers, the only restriction is: $ctg \alpha = 1/tg \alpha$.

We have defined \sin, \cos, tg, ctg for any angle from $[0^\circ, 360^\circ]$. Let's extend our definition.

At first we have to extend our domain, we have to consider the set of numbers $(360^\circ, +\infty)$.

Let's fix any number $\alpha > 360^\circ$. By definition, any angle $\alpha > 360^\circ$ is the combination: (k full counterclockwise rotations around the circle starting from the point A) and (the angle β), where both numbers k, β are taken from the representation $\alpha = 360^\circ \cdot k + \beta \parallel k \in \mathbb{N}, \beta \in [0^\circ, 360^\circ)$. Such representation is obviously unique for any number $\alpha > 360^\circ$.

For example, the angle $\alpha = 480^\circ$ is one full counterclockwise rotation and the angle $\beta = 120^\circ$. The angle $\alpha = 980^\circ$ is two full counterclockwise rotations and the angle $\beta = 240^\circ$.

Any angle $\alpha > 360^\circ$ defines some point B on the circle, with coordinates (x_B, y_B) . By definition:

$$\cos \alpha \equiv x_B \parallel \sin \alpha \equiv y_B \parallel tg \alpha \equiv \frac{\sin \alpha}{\cos \alpha} \parallel ctg \alpha \equiv \frac{\cos \alpha}{\sin \alpha} \parallel.$$

We have defined what is the angle $\alpha \in [0^\circ, +\infty)$ and its trigonometric functions.

Let's fix any number $\alpha < 0^\circ$. The negative angle α is the angle $|\alpha|$, which is built in the **clockwise** direction from the point A .

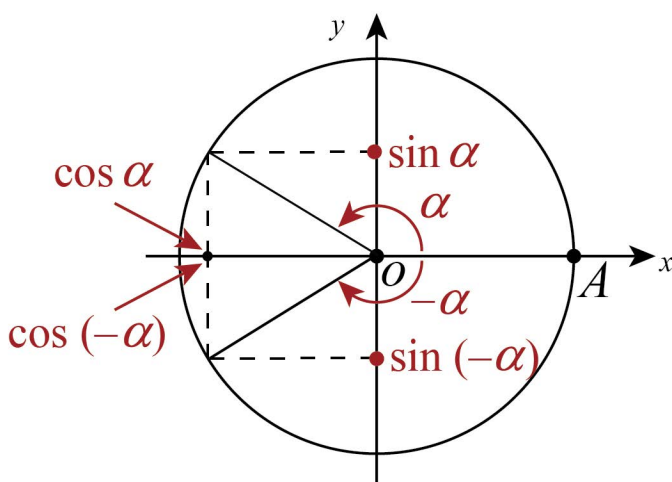
In particular, any negative angle $\alpha < -360^\circ$ is the combination of (k full **clockwise** rotations around the circle starting from the point A) and (some negative angle $-\beta \in (-360^\circ, 0^\circ]$).

Properties. [A] For any angle α , the points on the circle, which correspond to the angles α and $-\alpha$, are symmetric with respect to Ox , so these points have equal Ox -coordinates [pict9], then $\cos \alpha = \cos(-\alpha)$. These points also have opposite Oy -coordinates, then $\sin \alpha = -\sin(-\alpha)$.

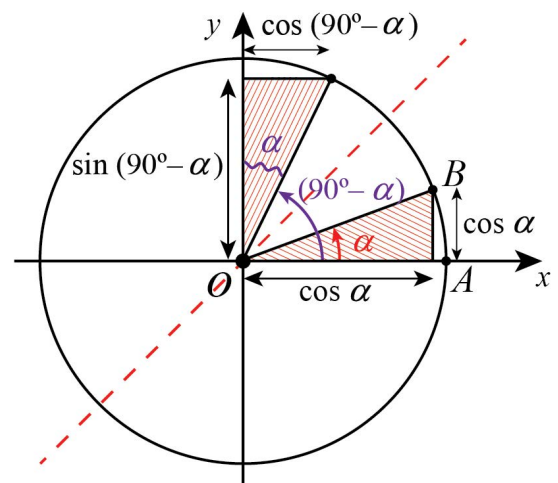
[B] For any angle α , the points on the circle, which correspond to angles α and $180^\circ - \alpha$ are symmetric with respect to Oy , therefore $\sin(180^\circ - \alpha) = \sin \alpha$ and $\cos(180^\circ - \alpha) = -\cos \alpha$.

[C] Let's fix any positive acute angle $\alpha \in [0^\circ, 90^\circ)$ and mark the angles α and $90^\circ - \alpha$ [pict10].

It's easy to build two equal right triangles, from their equality follows that $\sin \alpha = \cos(90^\circ - \alpha)$ and $\cos \alpha = \sin(90^\circ - \alpha)$. In fact these formulas are true for any angle α .



pict.9



pict.10

Really, it's easy to understand that for any angle α , the points on the circle, which correspond to angles α and $90^\circ - \alpha$, are always symmetric with respect to the angle bisector (red dashed line in [pict10]). The symmetry with respect to this bisector changes the places of Ox and Oy , from here follows the assertion we need.

From [A],[B],[C] we can deduce some trigonometric values. For example, we know that $\sin 45^\circ = \cos 45^\circ = 1/\sqrt{2}$, then from [A] follows that $\cos(-45^\circ) = \cos 45^\circ = 1/\sqrt{2}$ and $\sin(-45^\circ) = -\sin 45^\circ = -1/\sqrt{2}$ and from [B] follows that $\cos(135^\circ) = -\cos 45^\circ = -1/\sqrt{2}$ and $\sin(135^\circ) = \sin 45^\circ = 1/\sqrt{2}$.

In many cases it's more convenient to use "radians" instead of angles. Radians are defined in the next book.

Literature

1. Encyclopedia of elementary mathematics. Volume 1.
P.S Aleksandrov, A.I Markushevich, A. Hinchin. Leningrad, 1951.
2. Encyclopedia of elementary mathematics, Volume 3.
P.S Aleksandrov, A.I Markushevich, A. Hinchin. Leningrad, 1951.
3. Foundations of geometry, A.D Aleksandrov. Moscow, 1987.
4. Numbers and polynomials. I.V Proskuryakov. Moscow, 1965.
5. Course of differential and integral calculus, Volume 1. G.M. Fihtengolz. FizMatLit, 2001.
6. Mathematical Analysis. M.V Falalleev. Irkutsk 2013.
7. Mathematical Analysis. A.I. Kozko. MGU 2017
8. Lecture Course in Mathematical Analysis. V.I. Kolyada, A.A Korenovski. Odessa 2009.
9. Course of mathematical analysis. A.M. Ter-Krikorov, M.I. Shabunin. FizMatLit, 2001